Secure Web Gateway

Version 11.6

Hybrid Deployment Guide

Legal Notice

While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: support@trustwave.com

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Revision History

Version	Date	Changes
1.0	May 2012	MSC v2.0/SWG V10.2 Version release
1.1	December 2012	MSC V2.1/SWG V11.0 Version release
1.2	December 2013	MSC V2.2/SWG V11.5 Version release
1.3	November 2014	MSC V2.3/SWG V11.6 Version release

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or e-mail address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and checkbox names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in `Courier New 9 pt in blue` indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

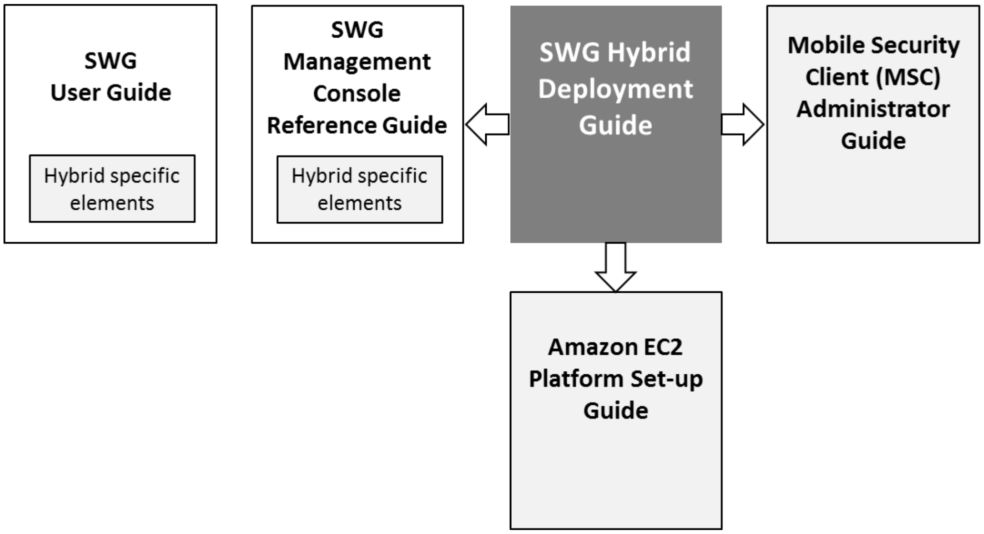
Notes, Tips, and Cautions

🔍	**Note**: This symbol indicates information that applies to the task at hand.
💡	**Tip**: This symbol denotes a suggestion for a better or more productive way to use the product.
❗	**Caution**: This symbol highlights a warning against using the software in an unintended manner.
❓	**Question:** This symbol indicates a question that the reader should consider.

Table of Contents

About this Guide

This guide is intended to help Secure Web Gateway (SWG) Administrators set up and configure a Trustwave SWG-Hybrid deployment. As well as providing essential background and insight, it supplements and coordinates use of standard SWG product documentation.



The Hybrid Deployment Guide assumes that you have a working knowledge of the Trustwave SWG product and an existing functioning SWG Policy Server and on-premise Scanning Server.

1 Introduction

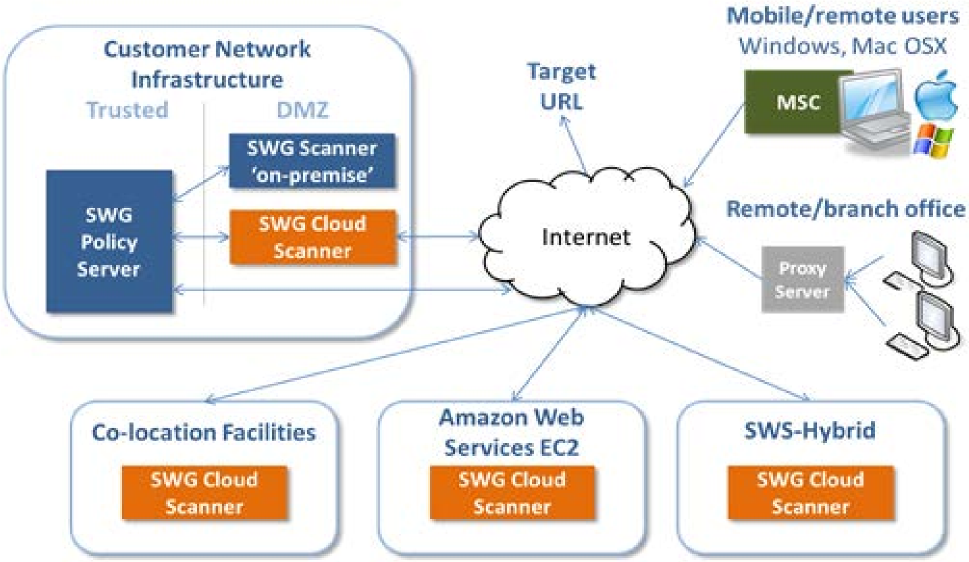
1.1 What is Hybrid Deployment?

Hybrid deployment is a feature of the Trustwave SWG product that extends Web filtering/security to Windows and Mac personal computer (PC) users when they are off-premise, i.e. connecting to the Internet from hotels, airports, Internet cafes, working from home or from remote offices. Hybrid deployment can also be used to secure remote offices that have a local Web proxy.

Note: For details of support for smartphones and tablets, see the *Mobile Device Support Technical Brief*.

For mobile/roaming users, the Hybrid involves installing a piece of client software on the PC, the **Trustwave Mobile Security Client** (MSC), and setting up one or more dedicated **SWG Cloud Scanners** that the client can authenticate with and securely route its Web traffic through. Remote/branch offices can be secured using the MSC on each PC or by using a local proxy server linked to a Cloud Scanner.

The Cloud Scanner systems can be deployed within the customer's own data centers, in co-location facilities, in Amazon Web Services EC2, or using Trustwave Secure Web Service Hybrid (SWS-Hybrid), as shown in the diagram below.



The aim is to position them as close to the mobile/remote user community as possible to ensure low latency connections and therefore a good Web browsing experience.

A typical deployment might include a Cloud Scanner at head office to cover home workers or visitors to the area, and one in each main geographical area of operation, e.g. Europe, APAC, US East and US West coast to cover travelling users and remote/branch offices.

As a mobile user moves to different locations, they will automatically use the Cloud Scanner that gives them the best performance (lowest latency). For example, if they are on-premise and an on-premise gateway is available they will use it - if they are on a business trip abroad then a scanner that gives the lowest latency will be used.

PCs connected using these scenarios are fully integrated into the policy enforcement, management and reporting provided by the Trustwave SWG product no matter where they are working from.

1.2 Why use SWG-Hybrid Deployment?

In summary, a Hybrid deployment of SWG can protect mobile/roaming and remote/branch office Personal Computer users:

- with the same command, control and reporting infrastructure as on-premise users
- while applying the same AUP and reporting as on-premise users
- allowing Web gateways to be placed close to where the users are (ensuring low latency)
- by reaching geographic locations that would otherwise be impractical
- without backhauling Web traffic to the HQ
- with multiple cloud scanner platform options: hardware appliance, virtual appliance, Amazon EC2, Trustwave SWS-Hybrid

Mobile/remote users are supported as a seamless extension of the existing SWG implementation.

1.3 Points to Consider

Three key items in this guide that should help simplify a deployment:

- Get an overview of the four step Hybrid Deployment process in How to Implement SWG-Hybrid, on page 18.
- Simplify planning by reading Deployment Decisions and Preparation, on page 19.
- SWG Policy Server Configuration workflow, summarized on page 26.

1.4 Terminology

The following terms are used throughout this user guide:

Term	Description
Cloud Load Balancer	A load balancer that is either deployed by a customer on the Amazon EC2 platform or by Trustwave on the Trustwave SWS-Hybrid platform.
EC2	Amazon Elastic Computer Cloud (Amazon EC2) http://aws.amazon.com/ec2/ is a Web service that provides resizable compute capacity in the cloud. It is used as a platform for the Trustwave SWG Cloud Scanner.
Cloud Proxy	Used to refer to both Cloud Scanners and Cloud Load Balancers.
Cloud Scanner	An SWG scanning server type designed to support mobile/roaming workers while being deployed in cloud based infrastructure such as Amazon EC2, Trustwave SWS-Hybrid or in an organization’s own private cloud infrastructure.
Elastic IP Address	Amazon EC2 Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An Elastic IP address is associated with your EC2 account and used against a specific Cloud Scanner Instance or Cloud Load Balancer instance.
Mac OS X	Apple Macintosh ("Mac") operating system.
MSC	Trustwave Mobile Security Client software installed on the user’s Personal Computer (Windows or Mac OS X) to redirect Web traffic to available SWG Cloud Scanners. Mobile Security Client; works with both SWG and WFR products.
PAC file	A Proxy Auto-Configuration (PAC) file defines how Web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. A PAC file contains a Java Script function "FindProxyForURL(url, host)".
PC	Personal computer; refers to both Microsoft Windows and Apple Mac based systems.
Mobile/remote user/computer	A laptop, home office desktop or otherwise non-static computer.
Region	A geographic region in which Cloud Scanners can be located.
SWG	Trustwave Secure Web Gateway product.
SWG Scanner or Scanning Server	A Trustwave SWG Scanner server installed in the corporate network.
SWG Policy Server	A Trustwave SWG Policy Server installed in the corporate network.

2 Deployment Scenarios

Hybrid deployments of SWG allow mobile/roaming users and remote/branch offices to be protected by using SWG Cloud Scanners and the Mobile Security Client software.

- **Cloud Scanners** are virtualized SWG Scanning Servers that are configured to support connections only from user computers running the Trustwave Mobile Security Client, or specifically defined proxy servers, for example in remote/branch offices. Cloud Scanners can be run on a choice of four different platforms depending on the target environment and management needs.

- The **Mobile Security Client** (MSC) is software that is installed on the computer endpoint and redirects Web traffic to the appropriate Cloud Scanner. The MSC enables identification, authentication and privacy of traffic between itself and the cloud scanner(s).

- The **SWG Policy Server** is, as with normal on-premise Scanning Server deployments, the central point of administration and control.

This section describes MSC End Point deployment and Cloud Scanner deployments. MSC and Cloud Scanner deployments can be mixed to produce the most appropriate Web security solution.

2.1 End Point Deployment

The most common use cases are:

1. Mobile/roaming workers using Mobile Security Client (MSC)
2. Remote/Branch office with PCs using MSC
3. Remote/Branch office with local proxy server

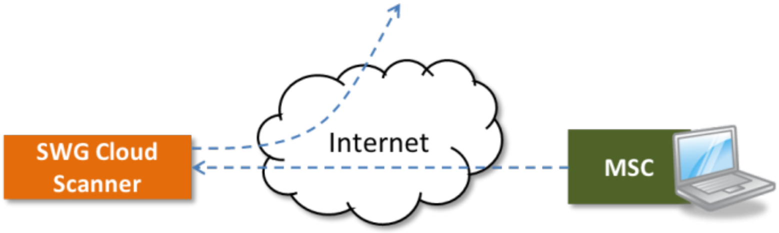
2.1.1 Mobile/Roaming Workers using Mobile Security Client (MSC)

Mobile/roaming workers have the MSC software installed on their PC (Windows or Mac). When the user is travelling and connects to the Internet from an external (non-company) network, for example hotel, airport, home office and so on, the client recognizes this and attempts to route Web traffic to the nearest available Cloud Scanner defined in its configuration.

Direct connection

No proxy and open firewall (or no firewall) between the client and the ISP, for example working from home using broadband or Dial-up over 3G.

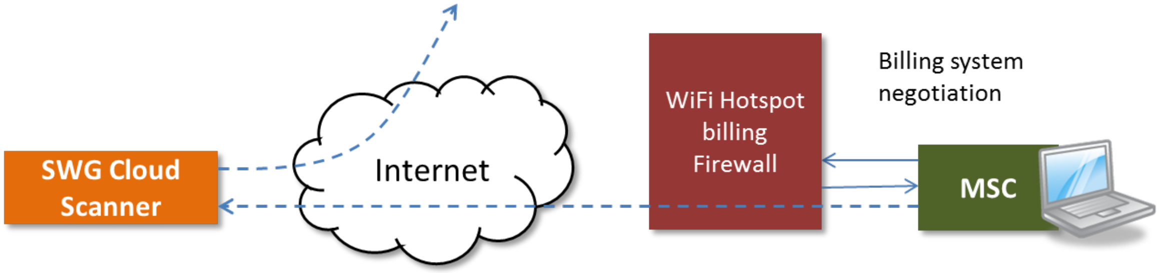
Traffic Flow: The MSC redirects Web requests from the PC browser to the Cloud Scanner proxy where the security policy is applied.



Wi-Fi Hotspot

Wi-Fi hotspots in locations such as airports, cafes, and hotels often use front end billing/registration systems that must be negotiated before receiving an Internet connection. The MSC is able to deal with these scenarios automatically.

Traffic Flow: The MSC first tries to reach the configured Cloud Scanner. On failing to do this it falls back to direct connection on port 80 which is intercepted by the Billing System firewall. Once the billing system has been negotiated by the user, the hotspot firewall opens up and the MSC is able to see the Cloud Scanner and automatically begins to redirect Web traffic to it so that security policy can be applied.



On-premise (headquarters)

When the mobile/roaming user returns to the office (i.e. on-premise) and connects from the secure zone of the company network, the MSC detects this and attempts to use the on-premise security solution; local SWG Scanning Server, local Web proxy or transparent mode SWG according to the configuration previously set. Alternatively, the configuration can be set via the SWG Policy Server, to allow the MSC to continue as though it were off-premise.

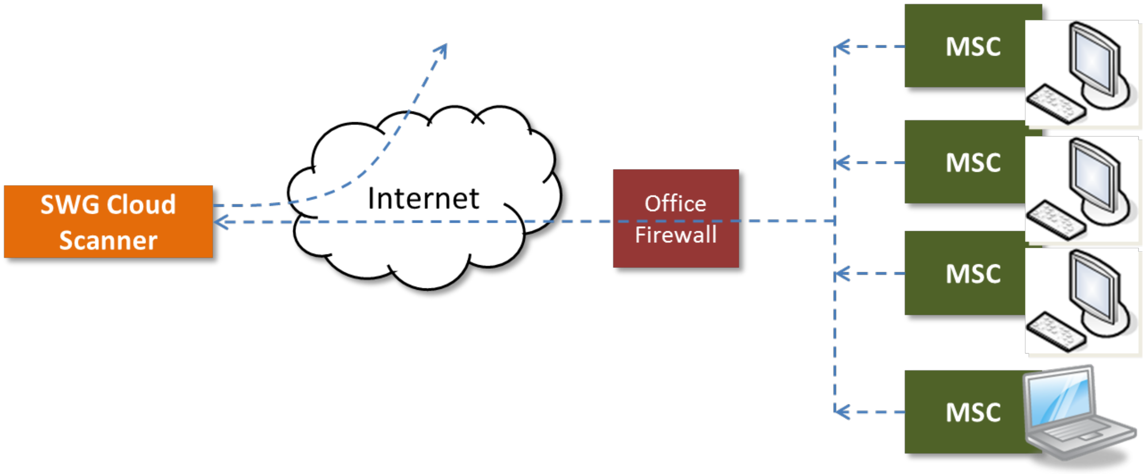
2.1.2 Remote/Branch Office with PCs Using MSC

All PCs can be installed with the MSC and Web traffic can be routed via the nearest Cloud Scanner in the same way as for the roaming user. Roaming users who visit the office will continue to operate as though they were roaming.

This is a good solution for offices where:

- geographic location makes deployment and support of local equipment difficult
- where a VPN connection back to the headquarters is not available
- connecting back to the headquarters would introduce too much latency
- there is no desire to backhaul Web traffic to the corporate HQ

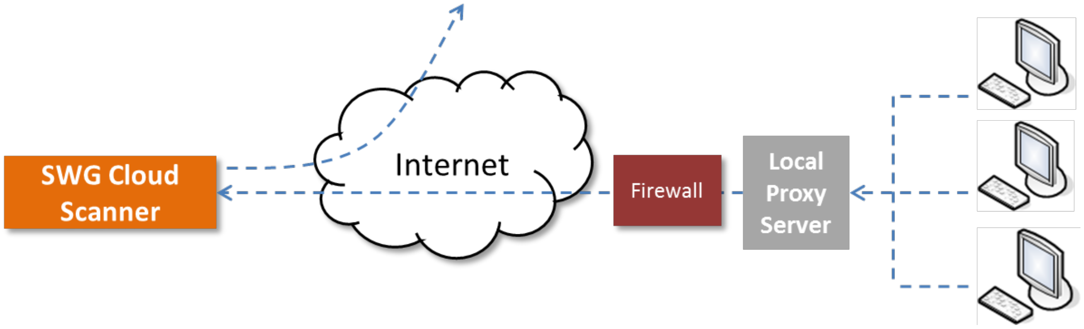
Traffic Flow: The MSC on each PC redirects Web traffic directly to the Cloud Scanner where the security policy is applied.



2.1.3 Remote/Branch Office with Local Proxy Server

In remote/branch offices where there is already a local proxy server, for example Microsoft ISS, it is not necessary for all PCs to run the MSC.

Traffic Flow: Each PC is configured to pass its Web traffic to the local proxy server. The proxy server is configured to forward this traffic to the Cloud Scanner where security policy is applied.



This topology has the advantage of easy setup and maintenance since the PCs do not need software to be installed. However, there are some caveats:

- HTTP traffic from the proxy server to the Cloud Scanner is **not** encrypted.
- There may be a reduction in the level of identification information available, making policy application and reporting less granular.
- The proxy may not be able to failover to another Cloud Scanner (in another Region) in the event of the first failing. This situation can be mitigated by the use of multiple Cloud Scanners and a Cloud Load Balancer in the same Region (see Cloud Scanner Deployment, page 14).
- Access to the Cloud Scanner by local proxy servers must be restricted to specific customer IP addresses or the security of the implementation is compromised.

If required, the proxy server scenario can be combined with PCs running MSC, for example where mobile/roaming workers come into a branch office to work for the day.

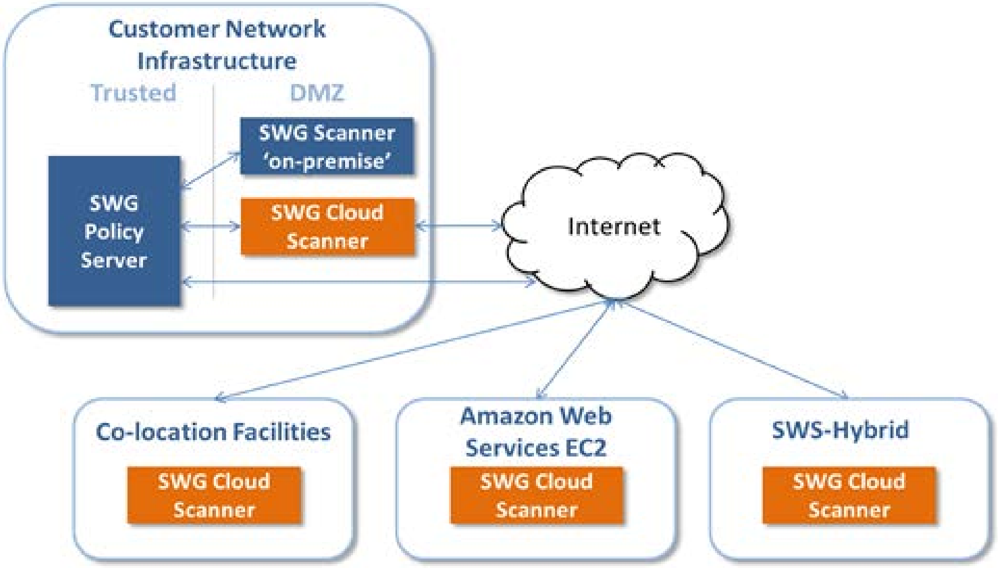
2.2 Cloud Scanner Deployment

Cloud Scanners can be deployed using four different platforms to match the customer's network environment. In general the aim is to locate Cloud Scanners close to the mobile/roaming users and remote/branch offices in order to minimize latency, thereby providing the best browsing experience.

1. Trustwave Hardware Appliance
2. Trustwave Virtual Appliance
3. Amazon Web Services EC2
4. Trustwave Secure Web Service Hybrid (SWS-Hybrid)

Cloud Scanners are controlled by and interact with the SWG Policy Server in the same manner, regardless of which platform they are deployed on.

Each of the cloud scanner platform options are represented in the illustration below (an on-premise SWG Scanner and SWG Policy Server are shown for context):



2.2.1 Customer Network Infrastructure (Private Cloud)

In this topology the Cloud Scanner is deployed on a DMZ on the customer's network infrastructure. This is a typical use case to support mobile/roaming users and remote/branch offices in the same country as the Cloud Scanner. This type of deployment typically has high speed network connectivity between the Cloud Scanner and the SWG Policy Server. This is sometimes termed a **Private Cloud** configuration.

2.2.2 Co-location Facility

Sometimes is it not possible to deploy a Cloud Scanner where it is needed; either the customer does not have a data center nearby or the other platform options, Amazon EC2 and Trustwave SWS-Hybrid, do not cover that area. In this situation a Co-location Facility deployment is recommended. The Cloud Scanner is implemented in a Co-location data center in the required location using customer owned/hired hardware (either Trustwave Hardware Appliance or Trustwave Virtual Appliance platforms). This is similar to the Customer Network Infrastructure deployment, but located instead in a business partner's data center.

2.2.3 Amazon Web Services EC2

An alternative to a Co-location Facility deployment is to use the Amazon Web Services EC2 cloud service. Special Trustwave SWG Cloud Scanner AMIs (Amazon Machine Images) are provided which can be used to create Cloud Scanner instances. This option takes away the effort of procuring, deploying, operating, and maintaining the underlying Cloud Scanner hardware platform and network connectivity. However, the customer will need to learn to use the Amazon EC2 environment.

Cloud Scanners can be placed in the following geographic Regions:

- APAC (Tokyo)
- APAC (Singapore)
- Europe (Eire)
- South America (Sao Paulo)
- US East (North Virginia)
- US West (California)
- US West (Oregon)
- APAC (Sydney)

Note: This option is **not** available for SWG Policy Servers.

2.2.4 Trustwave Secure Web Service Hybrid (SWS-Hybrid)

SWS-Hybrid is for customers who require a completely hands-off approach to the Cloud Scanner platform. Trustwave takes care of the platform set-up and maintenance using an IaaS provider such as Amazon. The customer can now focus on SWG policy management. The same geographic regions are covered as for the Amazon EC2 Cloud Scanner platform described above.

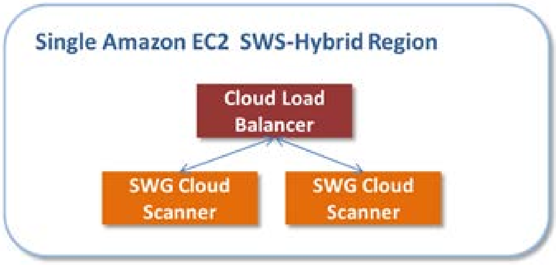
An SWS-Hybrid Cloud Scanner can often be implemented in as little as a few days making it ideal for fast deployment and where the logistics of deployment are difficult, e.g. in foreign countries.

Note: This option is **not** available for SWG Policy Servers.

2.2.5 Multi-Scanner and Load Balancer Deployment

In the on-premise and co-location scenarios the same load balancer methods as for the normal on-premise SWG Scanning Servers are used.

With Amazon EC2 and Trustwave SWS-Hybrid deployment platforms, if more than one Cloud Scanner is needed in a single geographic Region to increase user capacity, then a special Cloud Load Balancer instance is used.



IMPORTANT: A Region is typically split into Availability Zones which can enable geographic resilience.

Availability Zones are **not** currently supported by the Trustwave SWS-Hybrid platform.

For the Amazon EC2 platforms, be aware that placing Cloud Scanners in more than one Availability Zone in the same Region and linking them with a Load Balancer will lead to increased Amazon EC2 data transfers charges. For further details, consult the *Amazon EC2 Platform Set-up Guide* (Using Amazon EC2 as a platform for SWG Cloud Scanners).

2.3 Combining End Point and Cloud Scanner Deployments

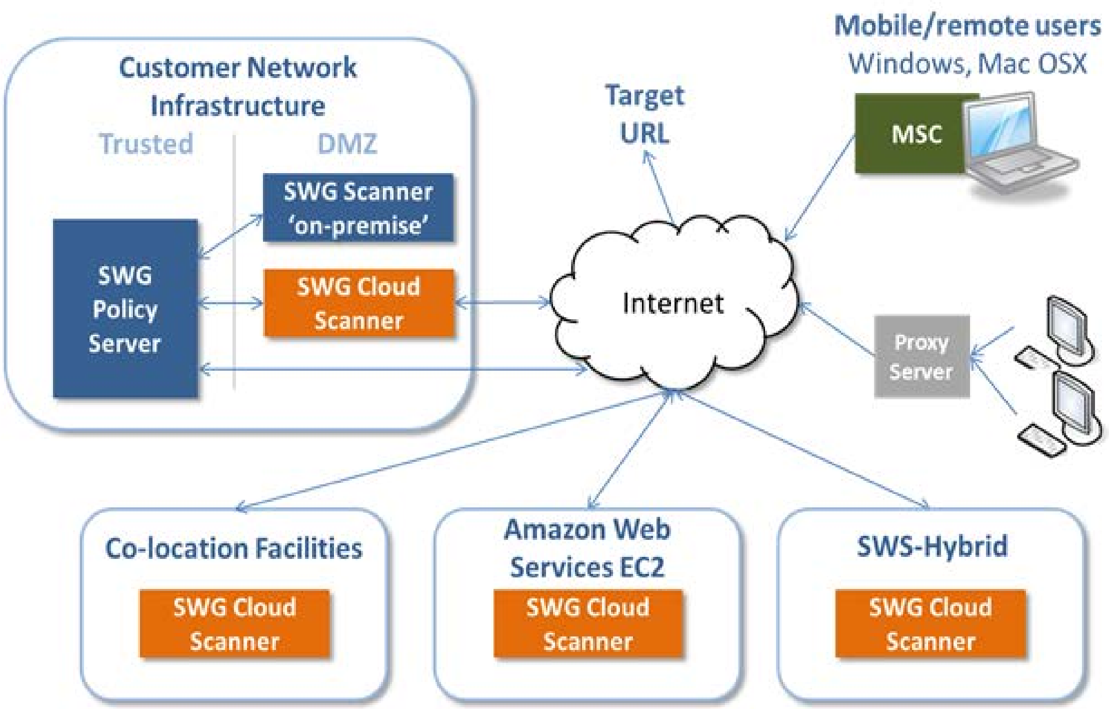
The SWG-Hybrid solution is very flexible:

- All end point deployments can be used with all Cloud Scanner deployments.
- Endpoint deployments can be mixed within an implementation.
- Cloud Scanner deployments can be mixed in the following manner:

Co Network Infrastructure		Co-Location Facility		Amazon EC2	SWS-Hybrid	
IBM	vmware	IBM	vmware	amazon web services	Trustwave	
Hardware Appliance	Virtual Appliance	Hardware Appliance	Virtual Appliance			Notes
✓	✓	✓	✓	✓	✗	Cannot combine EC2 and SWS-Hybrid
✓	✓	✓	✓	✗	✓	Cannot combine EC2 and SWS-Hybrid

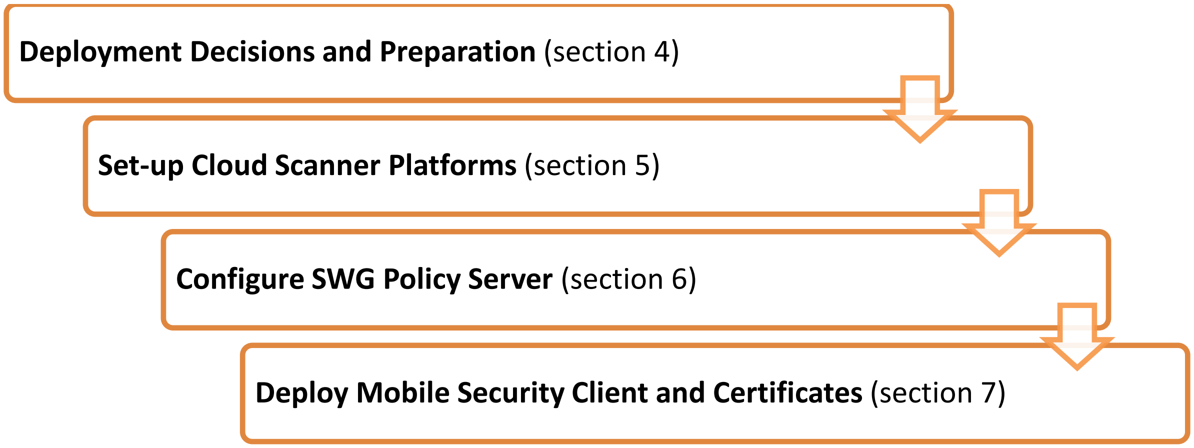
Note: Mixing Amazon EC2 (customer managed) and Trustwave SWS-Hybrid within a deployment is **not** permitted due to support complexities.

Each of the cloud scanner platform and end point options (excluding Cloud Load Balancers) are represented in the diagram below:



3 How to Implement SWG-Hybrid

Follow the four steps below to set-up an SWG-Hybrid deployment, but first ensure that a functioning SWG implementation, including Policy Server and on-premise Scanner, is already in place.



Deployment Decisions and Preparation (section 4)

Set-up Cloud Scanner Platforms (section 5)

Configure SWG Policy Server (section 6)

Deploy Mobile Security Client and Certificates (section 7)

Note: Although these steps are laid out sequentially for ease of reading, in practice there will be some level of recursion.

4 Deployment Decisions and Preparation

Before a Hybrid deployment is attempted, a number of decisions need to be made to determine:

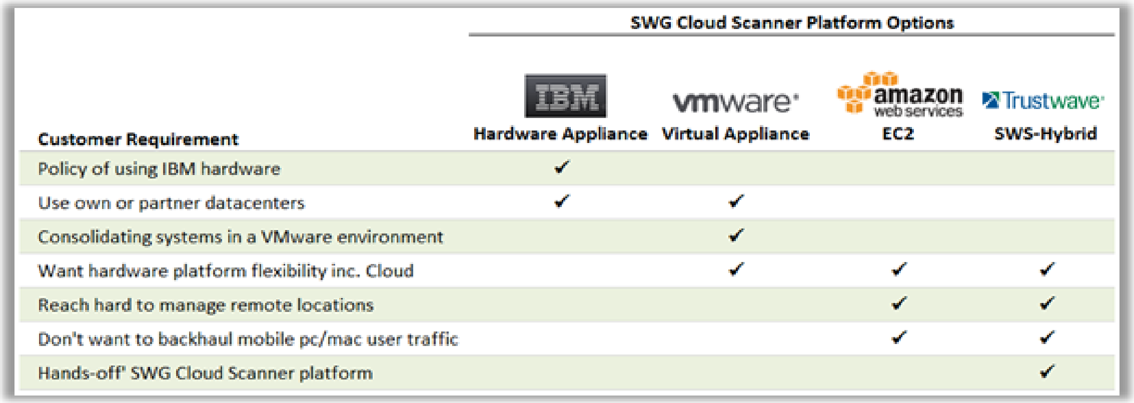
1. Cloud Scanner Platform Types
2. Cloud Scanner Platform Sizing and Load Balancers
3. Certificate Management Mode
4. Client types to be used: MS Windows and/or Mac OSX?
5. Client deployment method: email or external system?
6. PAC file deployment: Manual or from SWG Policy Server?

Each of these decision areas are explored below.

4.1 Cloud Scanner Platform Types

Cloud Scanners are virtualised SWG Scanning Servers that are configured to support connections only from user computers running the Trustwave Mobile Security Client, or specifically defined proxy servers, for example in remote/branch offices. Cloud Scanners can be run on a choice of four different platforms depending on the target environment and management needs. The platform choice will impact the set-up process that needs to be used later. However, the SWG Policy Server Configuration does not change.

Here is a summary of the platform types and their application and restrictions on combinations.



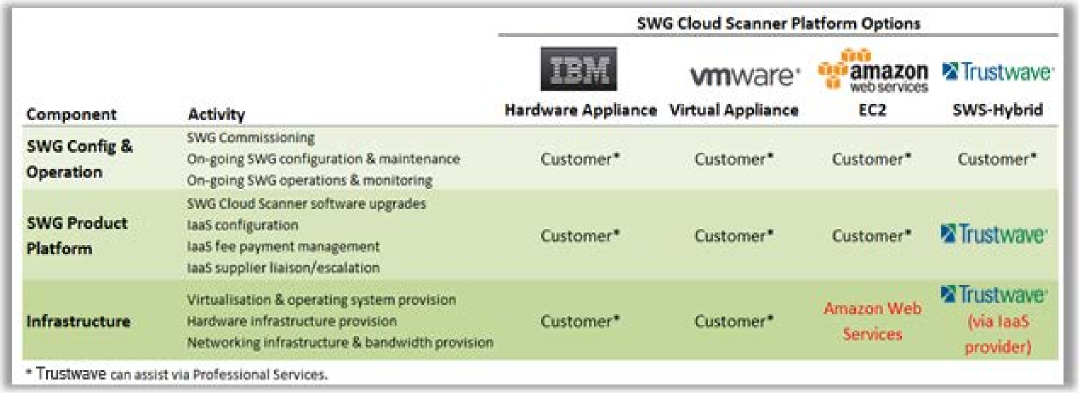
	SWG Cloud Scanner Platform Options			
Customer Requirement	IBM Hardware Appliance	vmware Virtual Appliance	amazon web services EC2	Trustwave SWS-Hybrid
Policy of using IBM hardware	✓			
Use own or partner datacenters	✓	✓		
Consolidating systems in a VMware environment		✓		
Want hardware platform flexibility inc. Cloud		✓	✓	✓
Reach hard to manage remote locations			✓	✓
Don't want to backhaul mobile pc/mac user traffic			✓	✓
Hands-off' SWG Cloud Scanner platform				✓

IMPORTANT: There are some restrictions in terms of which platforms can be combined in an implementation. See Combining End Point and Cloud Scanner Deployments, page17.

4.1.1 Cloud Scanner Platform Set-up Responsibilities

Secure Web Service-Hybrid cloud scanner platforms are set-up exclusively by Trustwave. All other cloud scanner platforms are the customer's responsibility, although of course assistance can be provided via Professional Services.

This is illustrated by the table below.

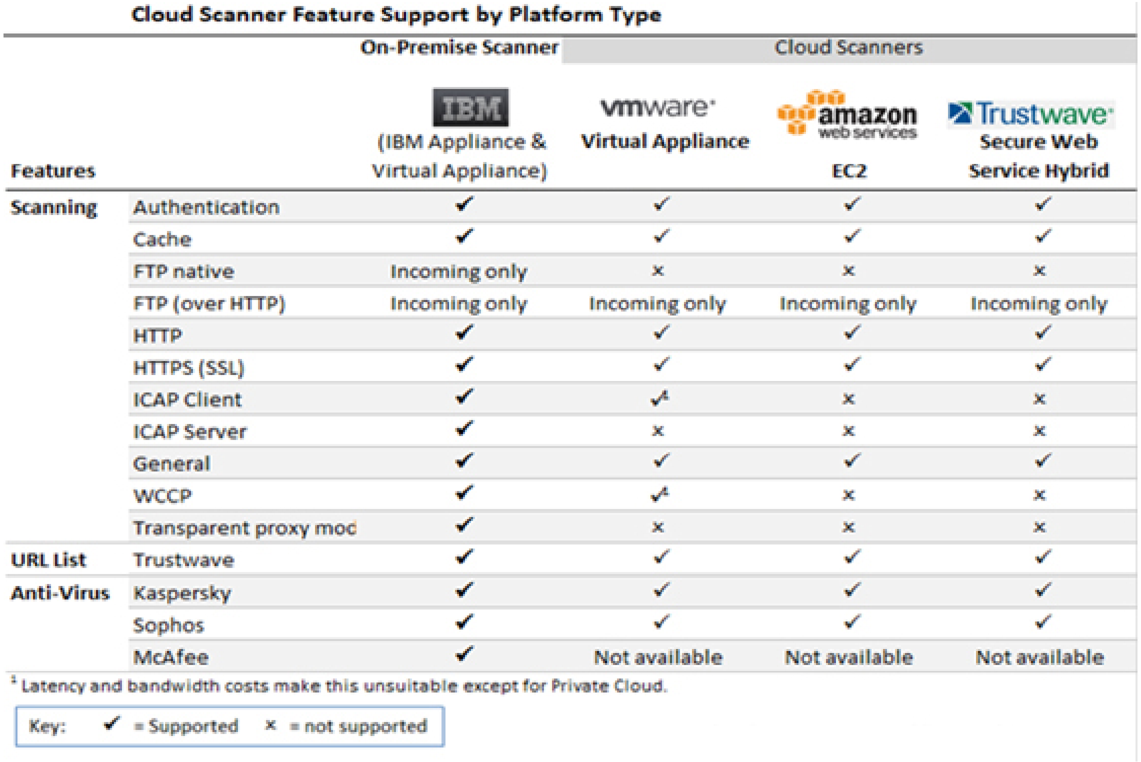


		SWG Cloud Scanner Platform Options			
		IBM	vmware	amazon web services	Trustwave
Component	Activity	Hardware Appliance	Virtual Appliance	EC2	SWS-Hybrid
SWG Config & Operation	SWG Commissioning On-going SWG configuration & maintenance On-going SWG operations & monitoring	Customer*	Customer*	Customer*	Customer*
SWG Product Platform	SWG Cloud Scanner software upgrades IaaS configuration IaaS fee payment management IaaS supplier liaison/escalation	Customer*	Customer*	Customer*	Trustwave
Infrastructure	Virtualisation & operating system provision Hardware infrastructure provision Networking infrastructure & bandwidth provision	Customer*	Customer*	Amazon Web Services	Trustwave (via IaaS provider)

* Trustwave can assist via Professional Services.

4.1.2 What functionality does each Cloud Scanner Platform support?

Not all SWG features make sense or can be used on a Cloud Scanner. This may be due to the need for high speed network connections, the impact on bandwidth costs when moving traffic around or simply that the function is not implemented. The following table summarizes the feature support of SWG 11.6:



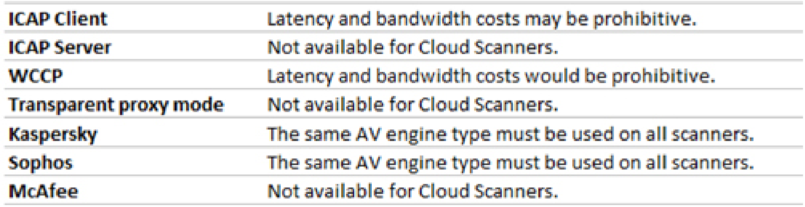
Cloud Scanner Feature Support by Platform Type

		On-Premise Scanner	Cloud Scanners		
		IBM (IBM Appliance & Virtual Appliance)	vmware Virtual Appliance	amazon web services EC2	Trustwave Secure Web Service Hybrid
Features					
Scanning	Authentication	✓	✓	✓	✓
	Cache	✓	✓	✓	✓
	FTP native	Incoming only	×	×	×
	FTP (over HTTP)	Incoming only	Incoming only	Incoming only	Incoming only
	HTTP	✓	✓	✓	✓
	HTTPS (SSL)	✓	✓	✓	✓
	ICAP Client	✓	✓[1]	×	×
	ICAP Server	✓	×	×	×
	General	✓	✓	✓	✓
	WCCP	✓	✓[1]	×	×
	Transparent proxy moc	✓	×	×	×
URL List	Trustwave	✓	✓	✓	✓
Anti-Virus	Kaspersky	✓	✓	✓	✓
	Sophos	✓	✓	✓	✓
	McAfee	✓	Not available	Not available	Not available

[1] Latency and bandwidth costs make this unsuitable except for Private Cloud.

Key: ✓ = Supported × = not supported

In addition, note the following:



ICAP Client	Latency and bandwidth costs may be prohibitive.
ICAP Server	Not available for Cloud Scanners.
WCCP	Latency and bandwidth costs would be prohibitive.
Transparent proxy mode	Not available for Cloud Scanners.
Kaspersky	The same AV engine type must be used on all scanners.
Sophos	The same AV engine type must be used on all scanners.
McAfee	Not available for Cloud Scanners.

4.2 Cloud Scanner Platform Sizing and Load Balancers

4.2.1 What size Cloud Scanner Platforms do I need?

Your Trustwave Sales Representative will be able to assist with sizing calculations for each platform type. When using Trustwave Secure Web Service Hybrid (SWS-H) this is all taken care of for you.

4.2.2 Are cloud-based Load Balancers needed?

For Amazon EC2 and Trustwave SWS-H platforms, if more than one Cloud Scanner is needed in a single geographic Region (e.g. Europe (Eire)), then a cloud based Load Balancer will be required. For Trustwave SWS-H platforms this will be taken care of for you. For Amazon EC2 platforms (where the customer uses their own Amazon EC2 account), consult the SWG Sizing Calculator for guidance on platform capacity and the need for Load Balancers.

IMPORTANT: If more than four Cloud Scanners are required in a single geographic Region (EC2 or SWS-Hybrid), contact Trustwave for assistance.

4.3 Certificate Management Mode

One of the most important decisions that impact the Hybrid set-up and operation process is the choice of client certificate management. Every end user of the Mobile Security Client requires a digital client certificate to be able to authenticate and identify with the SWG Cloud Scanners. SWG supports two approaches to this: either an external PKI system is used or the SWG Policy Server is used as an internal Certificate Authority.

	Creation	Distribution	Management
PKI Mode	PKI System	PKI System	PKI System
Internal Mode	SWG Policy Server is the Certificate Authority (CA)	SWG Email (attachment) or Export to Active Directory/Group Policy Object or similar	SWG Policy Server
Identification Only Mode	SWG Policy Server is the Certificate Authority (CA)	No distribution of user certificates	SWG Policy Server

4.3.1 PKI Mode (External PKI System)

If a PKI (Public Key Infrastructure) system is employed, certificate distribution will be taken care of completely outside of the SWG solution. Subsequent certificate management is also performed via the customer's PKI system. This choice of certificate management is global so far as the Hybrid configuration is concerned and will change the configuration screens available in the Cloud Configuration section of the SWG Policy Server.

4.3.2 Internal Certification Mode (Internal Certificate Authority)

When the Policy Server acts as the Certificate Authority (CA), it is also used as the certificate distribution point. Control over certificate validity (block, revoke, allow etc.) is then maintained on the SWG Policy Server.

Two distribution choices are available depending on the size of the deployment:

1. Internal Email Distribution

   For smaller implementations and proof of concept (POC) projects, the internal (SWG Policy Server) distribution mechanism can used to email certificates to each end user. When new users are added, certificates can optionally be automatically emailed to the end user.

   Default email templates are provided. However you may wish to consider tailoring these for your organization's particular needs.

   When using Internal Certification Mode, a password can be applied to the certificate installation process. Without the password the user cannot install the certificate. The password is defined as part of the client configuration step and distributed manually by the administrator to the target end users. (See Client Enforcement Settings - Client Configuration Tab, page 36.)

2. Export to Directory System (Active Directory)

   For larger deployments, certificates can be exported from the Policy Server management screens and then uploaded into a directory system such as MS Active Directory using an upload utility program. Subsequently, MS GPO is used to deliver the certificates to individual end users when they log in to their domain. A utility script and instructions are provided (see Appendix A).

Note: SWG version 11.0 and later and MSC version 2.1 and later allow for the use of a generic certificate. This can help with easier client set-up or proof of concept, or where user identification is not required.

4.3.3 Identification Only Mode (Internal Certificate Authority)

The policy server acts as the Certificate Authority for the server and generic user certificates only. There is no distribution of user certificates - identity information is automatically gathered from the system for the currently logged in user.

4.4 Client types to be used: MS Windows and/or Mac OSX?

If both Windows and Mac clients are to be used then consider that:

- Different code binary files are used for the Mobile Security Client on Windows and Mac.
- Different code distribution mechanisms may be required (e.g. GPO for Windows, Casper Suite for MAC).
- You may need to edit the default client deployment email templates.

4.5 Client deployment method: Email or External System?

The Mobile Security Client software is included as an individual executable file as part of the SWG product installation package. Updates to the client are provided as part of an overall SWG product version release, maintenance release or hotfix. In SWG v10.2 and later, client code versions are decoupled from the main product, in which case it may be supplied separately as an update package, as well as part of an overall SWG release.

Client deployment options are:

	Create Installer	Distribution	Management
PKI Mode	SWG Policy Server	G.P.O	Automatic (from SWG Policy Server)
Internal Mode	SWG Policy Server	SWG Email (link) or G.P.O	Automatic (from SWG Policy Server)
Identification Only Mode	SWG Policy Server	G.P.O	Automatic (from SWG Policy Server)

G.P.O = Group Policy Objects or similar

4.5.1 Client Deployment

Initial deployment of the MSC client software can be managed in two ways:

1. Internal distribution (Internal Certification Mode Only)

   The client can be distributed by using the built-in email feature of the Policy Server and then manually installed by the end user. A customizable email contains a download link and instructions for installing the MSC. The download location is chosen by the Administrator and can be placed on an internal shared directory, in a Web server requiring user/password, an FTP server, or even sent by email. This method is good for small/medium size and proof of concept deployments.

2. External software management system (e.g. G.P.O)

   In a Microsoft environment, an external software management system such as Microsoft Group Policy Objects can be used to deploy the MSC. The administrator makes the MSC install package available to the Group Policy Object (GPO) system, and end user systems are installed at domain login time. A silent install option is also available.

In a Mac OSX environment, the equivalent software distribution system, Casper Suite or even Apple Remote Desktop Management could be used. Alternatively the client code could be built into a master image of the client machines.

4.5.2 On-going Client Software Updates

The Administrator can enable or disable automatic client code updates globally. This increases control over the roll-out of client code (MSC).

If enabled, the MSC client code (binary) is updated automatically from the Cloud Scanner (via the Policy Server). The new client package is made available on the Policy Server via the Administrator. The MSC checks once per hour for code updates and if a newer version is available it will automatically download and execute it.

Client configuration updates are checked for once per hour. If the configuration version is the same or more recent than that on the client, a fresh copy is downloaded and applied, transparent to the end user.

In addition, client code auto-updates can be controlled by group membership, allowing the administrator to update MSC code by user group, and enabling the phased roll-out of new MSC versions.

Sales Engineers can also restrict MSC roll-out of new versions for test, pilot, or POC purposes.

4.5.3 Client Installation and Initial Configuration

The MSC installation process implements the MSC components and sets an initial default configuration as defined on the SWG Policy Server. Installation is performed under Administrator privileges.

System settings are automatically adjusted to use "proxy auto configuration script" and the URL location of the MSC PAC (Proxy Auto Configuration) file is set. Browsers and other applications that use the system setting will automatically use the PAC file. Other supported browser types will have their network settings adjusted directly by the MSC to point to the same PAC file. This setting of network configuration happens both at MSC install and periodically (approximately every fifteen seconds) whilst the MSC is running to help mitigate tampering.

4.6 PAC file deployment: Manual or from SWG Policy Server?

The Mobile Security Client uses a Proxy Auto Configuration (PAC) file. The SWG Policy Server automatically generates and maintains the PAC file based on the Cloud Configuration entered. There are two ways to manage the PAC file:

4.6.1 Automatic PAC File Management

The administrator can choose to distribute and update the PAC file automatically via the SWG Policy server. The Mobile Security Client will periodically check for updated PAC file. Switch this function on by navigating to the **Administration | Cloud Configuration – Client Configuration** tab and selecting the **Enforce PAC file usage via the Mobile Security Client** option.

4.6.2 On-Premise PAC File Option

Administrators can optimize MSC configuration by using the customer's standard PAC file when on-premise and the SWG-maintained PAC file when off-premise.

5 Setting Up Cloud Scanner Platforms

Cloud Scanner platforms should be set-up before attempting to configure the SWG Policy Server. The set-up of each Cloud Scanner platform type requires a different approach - instructions can be found as follows:

IMPORTANT: Before continuing, ensure that you have read Section 4, **Deployment Decisions and Preparation**.

5.1 Trustwave SWG Hardware Appliance

For instructions on how to set-up a Trustwave SWG Hardware Appliance, see the following references:

1. To build the SWG scanner platform: *SWG Set-up Guide*.
2. To convert the platform to an SWG Cloud Scanner*: SWG User Guide* Procedure: Defining a Private Cloud Scanner.

5.2 Trustwave SWG Virtual Appliance

For instructions on how to set-up a Trustwave SWG Virtual Appliance, see the following references:

1. To build the SWG scanner platform: *SWG Set-up Guide*.
2. To convert the platform to an SWG Cloud Scanner: *SWG User Guide* Procedure: Defining a Private Cloud Scanner.

5.3 Trustwave Secure Web Services Hybrid (SWS-H)

Set-up of the Trustwave SWS-Hybrid platform is performed exclusively by Trustwave staff – please ask for assistance.

5.4 Amazon Web Services EC2 Platform Set-up

Refer to the Trustwave document: *Amazon EC2 Platform Set-up Guide* (Using Amazon EC2 as a platform for SWG Cloud Scanners).

6 Configuring the SWG Policy Server

6.1 Workflow for Configuring the SWG Policy Server for Hybrid Deployment

The recommended sequence of steps needed to configure the SWG Policy Server with a hybrid deployment, i.e. using Cloud Scanners and Mobile Security Client, is detailed below. The main steps (What) are on the left of the table, the SWG Management Console screen needed (How) is then listed followed by the activities undertaken (Why). Each step is detailed in the following sections.

IMPORTANT: In this deployment guide we focus on the essential configuration details and provide additional background to help provide a better understanding of the overall process of SWG-Hybrid Deployment. More detailed procedures for using each of the SWG Management Console screens are available in the *SWG Management Console Reference Guide*.

Table: SWG Policy Server Configuration Work Flow			
	Deployment Step	**SWG Management Console Screen**	**Explanation**
General Set-up			
	Mail Server	**Mail Server Screen** (Administration | System Settings | Mail Server)	Configure email servers settings to ensure that the SWG can send client provisioning emails. This step may already have been completed in existing SWG implementations.
	Cloud Scanners Definition and Connection	**SWG Devices Screen** (Administration | System Settings | SWG Devices)	Define and connect the previously built SWG Cloud Scanners to the SWG.
Cloud Configuration			
	Choose Certificate Management Mode **Note**: Available Cloud Configuration screens will vary according to the choice made.	**Cloud Configuration** (Administration | Cloud | Certificate Mgmt Mode)	Choose **Internal Certification** (The Policy Server acts as Certificate Authority), or **Enterprise PKI** (client certificates are managed by an external PKI system). or **Identification Only** (The Policy Server acts as the Certificate Authority for the server and generic user certificates only)

Table: SWG Policy Server Configuration Work Flow

	Deployment Step	SWG Management Console Screen	Explanation
	Cloud Configuration (Internal Certification Mode)		
	Internal Certification Mode Certificate Management	**CA Management Tab** (Administration | Cloud | Certificate Management)	Determine the Certificate Authority as Internal or External. If internal, generate server, generic, and user certificates.
	Network and URL exclusions	**Bypass Tab** (Administration | Cloud | Configuration)	Define those addresses that should be excluded (bypassed) from scanning and for which the user will connect directly to the Internet.
	On-premise settings	**Proxies (On-premise) Tab** (Administration | Cloud | Configuration)	Configure On-premise Proxies and define how to determine when the client is on-premise vs. off-premise.
	Communications ports	**Proxies (Cloud) Tab** (Administration | Cloud | Configuration)	Configure Cloud Scanners (Proxies) communications port numbers.
	Client enforcement settings	**Client Configuration Tab** (Administration | Cloud | Configuration)	Client enforcement options and PAC file management options. Uninstall warning message text definition.
	Client provisioning settings	**Provisioning Tab** (Administration | Cloud | Configuration)	Define where to find client installers. PAC file download option for manual PAC file management. Mobile Security Client installer downloads for Windows and Mac OSX.
	Email template configuration	**Email Template Screen** (Administration | Cloud)	Customize the text of the client and/or client certificate provisioning emails.

Table: SWG Policy Server Configuration Work Flow

	Deployment Step	SWG Management Console Screen	Explanation
	Cloud Configuration (PKI Mode)		
	Choosing PKI mode causes changes to the available configuration screens. Where the configuration tabs are the same as for Internal mode use this guide, otherwise refer to the *SWG Management Console Reference Guide*	**Certificate Management Tab** (Administration | Cloud | Certificate Management)	Automatically generate the CA Certificate, Server Certificate and Generic Certificate. SWG acts as the Certificate Authority to issue the cloud scanner certificates and the generic certificate.
		CRL Handling Tab - for PKI Mode only. (Administration | Cloud | Certificate Management)	Specify the location of the CRL list and an optionally a schedule for automatically retrieving that latest CRL list.
		Bypass Tab - same as Internal Certification Mode. **Proxies (On-premise) Tab** - same as Internal Certification Mode. **Proxies (Cloud) Tab** - same as Internal Certification Mode. **Provisioning Tab** – different for PKI Mode. **Client Configuration Tab** – different for PKI Mode. **Email Template Screen** – not needed in PKI Mode.	
Cloud Configuration (Identification Only Mode)			
	Choosing Identification Only mode causes changes to the available configuration screens.	**Certificate Management Tab** (Administration | Cloud | Certificate Management)	Automatically generate the CA Certificate, Server Certificate and Generic Certificate. SWG acts as the Certificate Authority to issue the cloud scanner certificates and the generic certificate.

Table: SWG Policy Server Configuration Work Flow

	Deployment Step	SWG Management Console Screen	Explanation
	Where the configuration tabs are the same as for Internal mode use this guide, otherwise refer to the *SWG Management Console Reference Guide*	**Bypass Tab** - same as Internal Certification Mode. **Proxies (On-premise) Tab** - same as Internal Certification Mode. **Proxies (Cloud) Tab** - same as Internal Certification Mode. **Provisioning Tab** – Same as PKI Mode. **Client Configuration Tab** – same as Internal Certification Mode. **Email Template Screen** – not needed in Identification Only Mode.	
User Management			
	Cloud Users and Groups	**Users/User Groups Screen** (Users)	Define Users and User Groups (including LDAP) that will use the Cloud Scanners (Proxies).
	Client certificates management (Internal Certification Mode)	**Cloud User Certificate Management** (Users)	On-going management of client certificates (i.e. issue, revoke, export etc.) when the SWG is working in Internal CA mode.

6.2 General Set-up

6.2.1 Mail Server

Note: This step may have already been completed in existing SWG deployments.

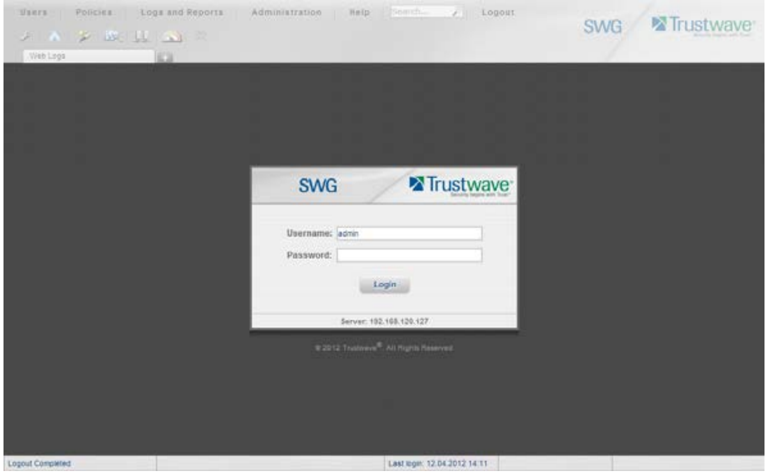
This is a necessary and important step when using **Internal Certification Mode.** Email is used to distribute Client Installation packages, client certificates and other Cloud related notification emails.

Refer to the *SWG Management Console Reference Guide* - Mail Server section for details on how enter the configuration.

6.2.2 Cloud Scanner Definition and Connection

Login to the SWG Policy Server

Navigate to the Secure Web Gateway Management Console and login.



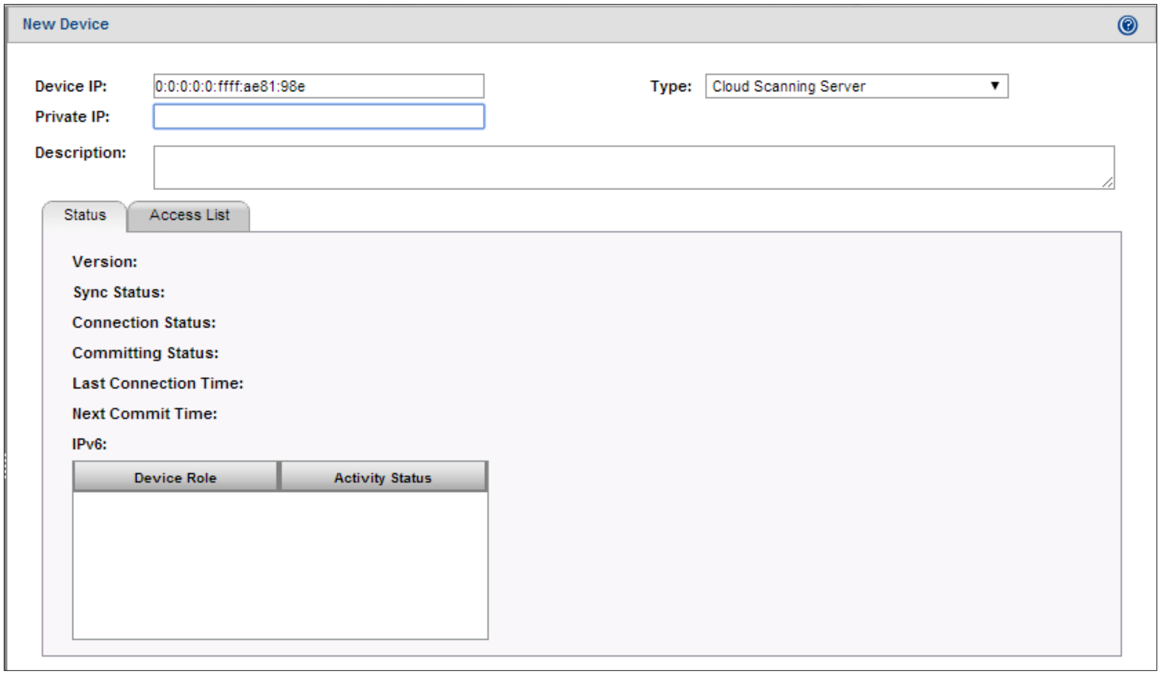
Username: admin
Password:
Server: 192.168.120.127
Logout Completed
Last login: 12.04.2012 14:11

To link a Cloud Scanner to the Policy Server:

1. Navigate in the Management Console to **Administration | System Settings | SWG Devices**.
2. Right-click the relevant Device Group, and select **Add Device**.
3. Select **Cloud Scanning Server** in the **Type** drop down list.
4. In the Device IP field, enter the Cloud Scanner IP.

WARNING: If using Amazon EC2 instances or Trustwave SWS-Hybrid Cloud Scanner platforms it is **highly recommended** that the Amazon EC2 **Elastic IP Address** is used. If a Load Balancer is also being used in EC2, then it **must** have an Elastic IP address.

5. In the **Private IP** field, enter the private IP.


New Device

Device IP: 0:0:0:0:0:ffff:ae81:98e

Private IP:

Type: Cloud Scanning Server

Description:

6. Repeat steps 1 to 5 for each new Cloud Scanner.

7. Click **Save**. Click ✓ to commit the changes.

8. Wait for policy distribution to complete.

Note: The initial connection time depends on the speed of the link between the SWG Policy Server and the Cloud Scanners. Around 30-40 minutes is typical.

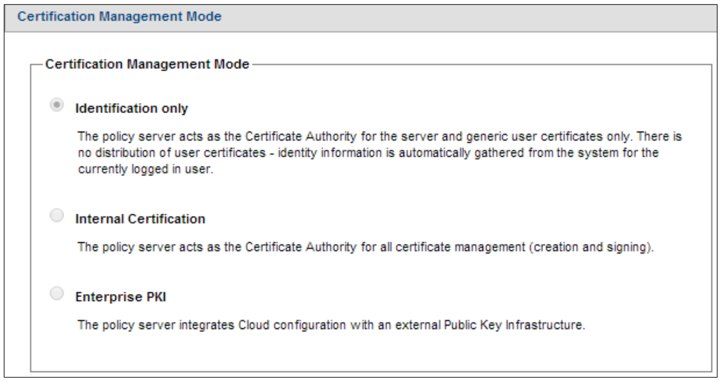
Tip: It is not possible to directly determine the scanner status during this period other than checking the sync indicator on the SWG Devices screen. However, in the System Logs viewer it is possible to see when synchronization with a certain scanner started and ended.

6.2.3 Choose Certificate Management Mode

IMPORTANT: The work flow sequence changes depending on whether an external PKI (Public Key Infrastructure) system is being used to manage client certificates (**PKI Mode**) or the SWG Policy Server is to be used as the certificate authority (**Internal Certification Mode**). See Deployment Decisions and Preparation, page 19, for a more detailed explanation**.**

To set the Certificate Management Mode:

1. Navigate to **Administration | Cloud | Certificate Mgmt Mode** and click **Edit**.
2. Select the **Internal Certification**, **Enterprise PKI**, or **Identification only** option.
3. Click **Save**.



Certification Management Mode

Certification Management Mode

● **Identification only**

The policy server acts as the Certificate Authority for the server and generic user certificates only. There is no distribution of user certificates - identity information is automatically gathered from the system for the currently logged in user.

○ **Internal Certification**

The policy server acts as the Certificate Authority for all certificate management (creation and signing).

○ **Enterprise PKI**

The policy server integrates Cloud configuration with an external Public Key Infrastructure.

6.3 Cloud Configuration - Internal Certification Mode

In Internal Certification Mode (or Internal Mode), the Policy Server acts as the Certificate Authority for all certificate management (creation and signing), issuing the cloud scanner certificates and the generic certificate.

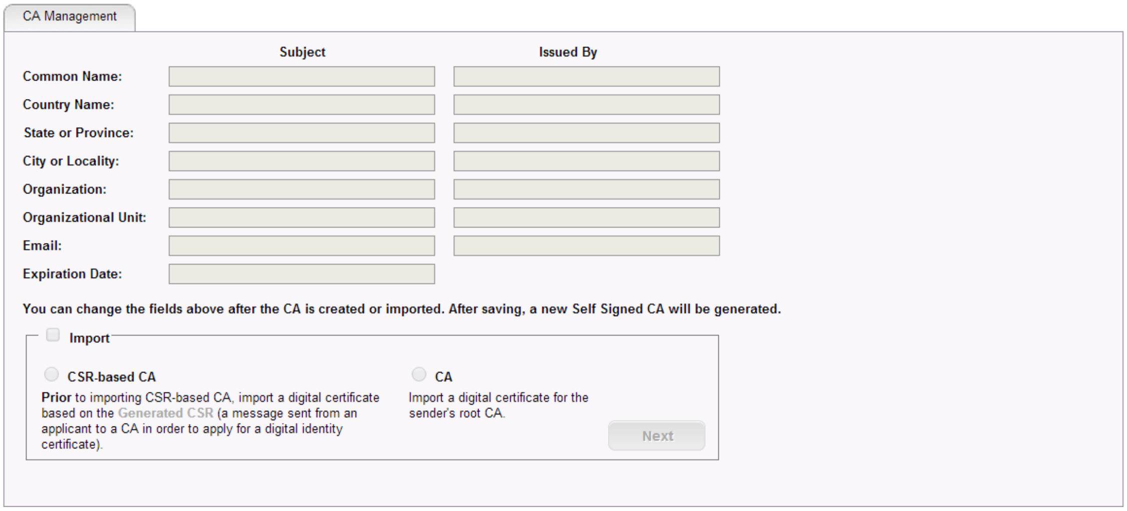
In Internal mode, you designate which users are cloud users, and manage users' certificates and certification status.

6.3.1 Certificate Management

Go to **Administration | Cloud | Certificate Management**.

The CA Management screen defines the Certificate Authority required for the creation and signing of all the certificates used in the Cloud environment (server certificates, cloud scanner certificates, the generic certificate, and mobile worker certificates).

For detailed instructions, see the *SWG Management Console Reference Guide*. For details of the methods available for Client Certificates export and distribution, see Certificate Deployment, page 46.



	Subject	Issued By
Common Name:		
Country Name:		
State or Province:		
City or Locality:		
Organization:		
Organizational Unit:		
Email:		
Expiration Date:		

You can change the fields above after the CA is created or imported. After saving, a new Self Signed CA will be generated.

□ Import

○ CSR-based CA

Prior to importing CSR-based CA, import a digital certificate based on the Generated CSR (a message sent from an applicant to a CA in order to apply for a digital identity certificate).

○ CA

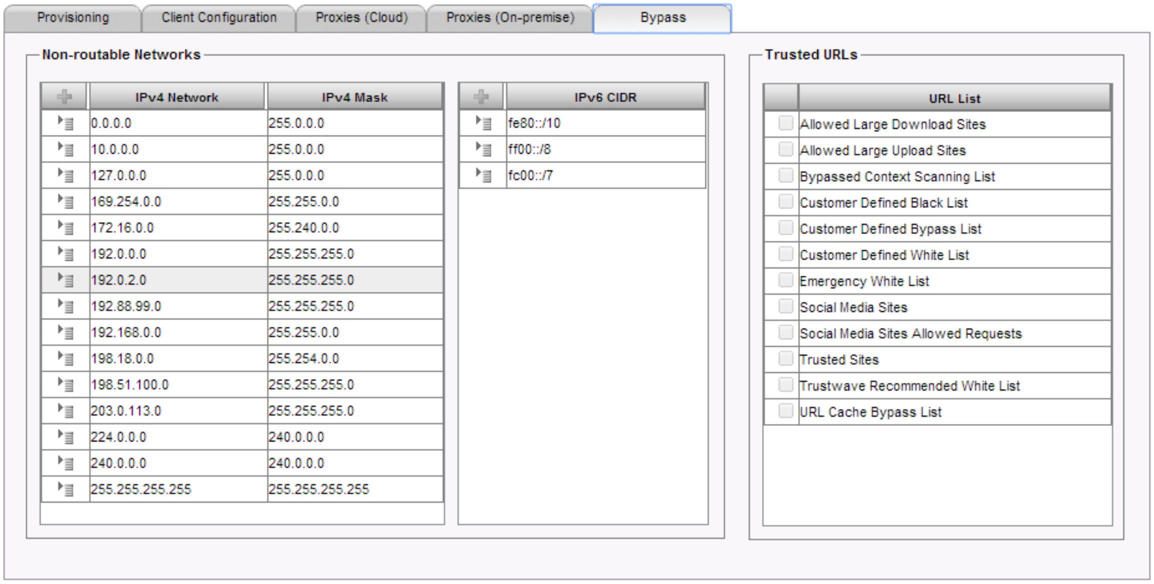
Import a digital certificate for the sender's root CA.

6.3.2 Network and URL Exclusions - Bypass Tab

Go to **Administration | Cloud | Configuration**.

The **Bypass** tab is used to define those addresses that should be excluded (bypassed) from scanning and for which the user will connect directly to the Internet. The tab includes the following fields:

- **Non-Routable Networks**: This table shows all networks or domains (IPs) to bypass while using Mobile Security Client with Cloud proxy or on-premise proxy.
- **Trusted URLs**: Choose the URLs that you want the Cloud proxy to bypass. Allow the organization to bypass certain URLs that the administrator deems safe (for example, Microsoft Update etc.).



Non-routable Networks

IPv4 Network	IPv4 Mask
0.0.0.0	255.0.0.0
10.0.0.0	255.0.0.0
127.0.0.0	255.0.0.0
169.254.0.0	255.255.0.0
172.16.0.0	255.240.0.0
192.0.0.0	255.255.255.0
192.0.2.0	255.255.255.0
192.88.99.0	255.255.255.0
192.168.0.0	255.255.0.0
198.18.0.0	255.254.0.0
198.51.100.0	255.255.255.0
203.0.113.0	255.255.255.0
224.0.0.0	240.0.0.0
240.0.0.0	240.0.0.0
255.255.255.255	255.255.255.255

IPv6 CIDR
fe80::/10
ff00::/8
fc00::/7

Trusted URLs

	URL List
□	Allowed Large Download Sites
□	Allowed Large Upload Sites
□	Bypassed Context Scanning List
□	Customer Defined Black List
□	Customer Defined Bypass List
□	Customer Defined White List
□	Emergency White List
□	Social Media Sites
□	Social Media Sites Allowed Requests
□	Trusted Sites
□	Trustwave Recommended White List
□	URL Cache Bypass List

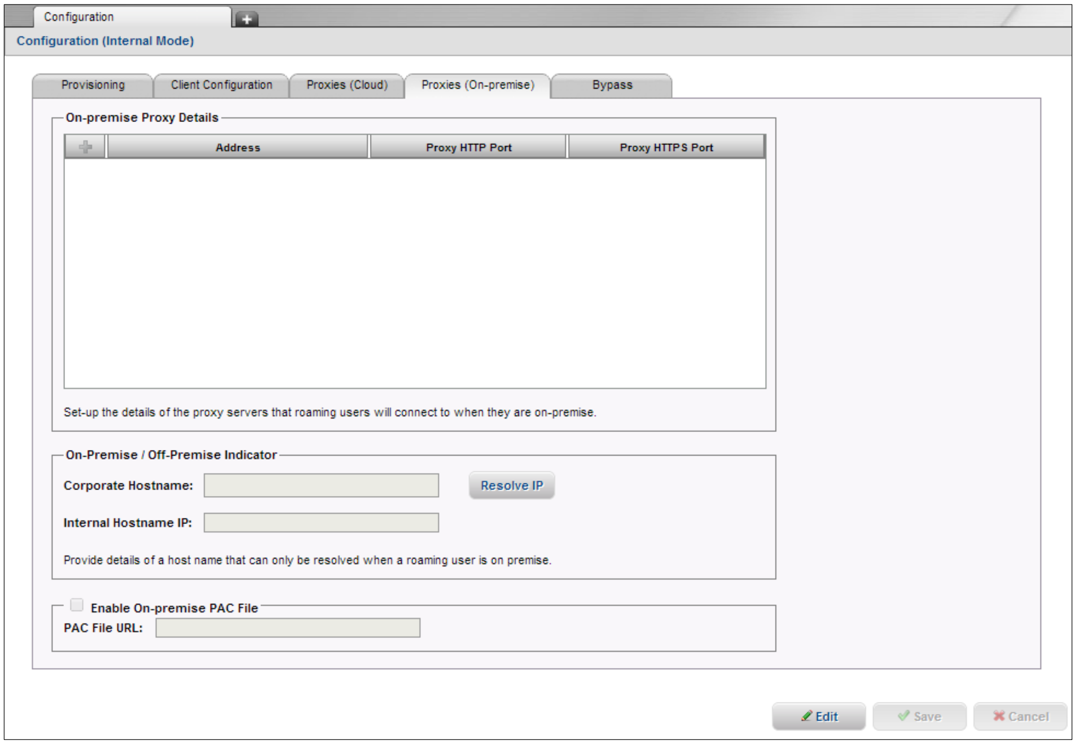
6.3.3 On-premise Settings - Proxies (On-premise) Tab

Go to **Administration | Cloud | Configuration**.

Tip: *SWG Management Console Reference Guide* location: Chapter 5, Cloud Configuration in Internal Certification Mode, **Proxies (On-premise) Tab.**

The Proxies (On-premise) tab has the following functions:

- To define Web proxies that exist within the customer network and are to be used when a mobile user is working "on-premise".
- To define when a mobile user is on-premise and when they are off-premise. This is achieved by defining a Corporate Hostname that can only be resolved to the defined Internal Hostname IP address when the user is "on-premise". The Mobile Security Client will use this information to connect either to an on-premise proxy or a Cloud Proxy (i.e. Cloud Scanner).
- To enable administrators to optimize MSC configuration by using the customer's standard PAC file when on-premise and the SWG-maintained PAC file when off-premise.



Set-up the details of the proxy servers that roaming users will connect to when they are on-premise.

Provide details of a host name that can only be resolved when a roaming user is on premise.

Note: The PAC file generated by the SWG Policy Server will include instructions to use the local proxy, if resolvable, as it recognizes you are within the local network. If the corporate hostname is not resolvable to the configured IP, it will use the nearest defined Cloud Scanner (proxy) available.

To enter On-Premise Proxy Details:

1. Click the **Add** icon and add the on-premise proxy details. There are two scenarios to consider depending on the SWG deployment type:
    - **Transparent Mode (implicit Proxy):** If a transparent mode deployment has been used for the on-premise proxy, i.e. no proxy details used at the PC end, then do **not** add any **on-premise proxy details**.
    - **Explicit proxy:** If the on-premise proxy (or load balancer) is used by pointing to it explicitly from the PC then add the IP address, HTTP and HTTPS ports for each one.
2. Repeat step 1 for each on-premise proxy.
3. If required, you can adjust the default cloud scanner by increasing or decreasing the priorities of cloud scanner entries.

To enter On-Premise/Off-Premise Indicator details:

Note: This is effectively an indicator that allows the Mobile Security Client to determine whether it is on or off-premise.

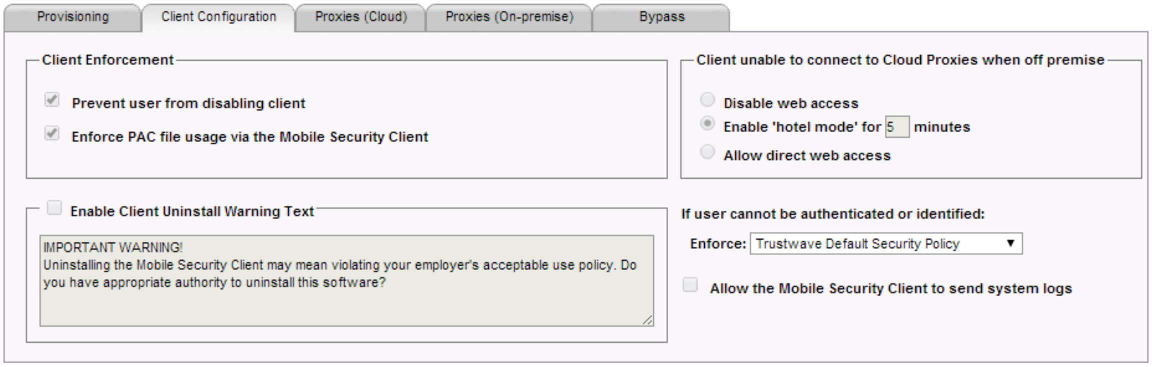
1. Enter the **Corporate Hostname** to be used as the on/off-premise indicator.
2. Enter the **Internal hostname IP** that the **Corporate Hostname** will resolve to, or click the **Resolve IP** button.
3. Test the on/off-premise indicator by selecting the **Resolve IP** button.

IMPORTANT: The administrator must ensure that the Corporate Hostname is resolvable with the supplied Internal Hostname IP only when on-premise. When the user is outside of the corporate network the corporate hostname should **not** be resolvable.

6.3.4 Client Enforcement Settings - Client Configuration Tab

Go to **Administration | Cloud | Configuration**.

The Client Configuration tab allows you to define how use of the client software is enforced.



Client Enforcement

☑ Prevent user from disabling client

☑ Enforce PAC file usage via the Mobile Security Client

Client unable to connect to Cloud Proxies when off premise

○ Disable web access

● Enable 'hotel mode' for 5 minutes

○ Allow direct web access

□ Enable Client Uninstall Warning Text

IMPORTANT WARNING!
Uninstalling the Mobile Security Client may mean violating your employer's acceptable use policy. Do you have appropriate authority to uninstall this software?

If user cannot be authenticated or identified:

Enforce: Trustwave Default Security Policy

□ Allow the Mobile Security Client to send system logs

6.3.4.1 Client Enforcement

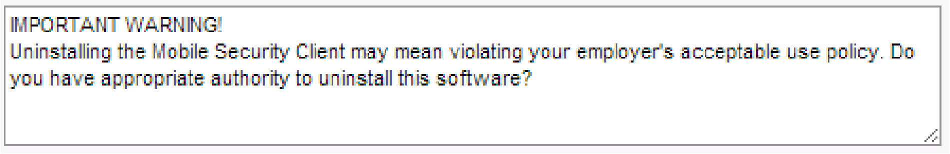
- **Prevent user from disabling client:** Enabling this check box ensures that the user cannot disable the agent in the browser, thereby allowing surfing through a Trustwave agent only.

Note: This option takes effect only in conjunction with the **Prevent user from disabling Mobile Security Client** option set against the user groups (see Cloud Users and Groups (Internal Certification Mode), page 44). That is, switch on the capability in the Client Provisioning Tab, and then apply it to specific users in the User /User Groups tab.

- **Enforce PAC file usage via the Secure Web Service Agent:** This is key to correct operation of the client. Enabling this check box assures that the PAC file being used is a Trustwave PAC file, automatically generated, maintained and distributed to the Mobile Security Client. Administrators should keep this box unchecked if a proprietary PAC file is used. See also Section 6.3.6.3, Download PAC File.

6.3.4.2 Enable Client Uninstall Warning Text

Enable Client Uninstall Warning Text: When enabled, a warning message can be presented to the user if they attempt to uninstall the Mobile Security Client. The idea is to make the user fully aware of what they are attempting to do while linking this to the fact that they may be contravening their employees acceptable use policy - which may have a set of consequences. A default message (shown below) is provided, however this can be customized as required.



IMPORTANT WARNING!
Uninstalling the Mobile Security Client may mean violating your employer's acceptable use policy. Do you have appropriate authority to uninstall this software?

6.3.4.3 Client Unable to Connect to Cloud Proxies when Off-premise

These options enable the administrator to control how the MSC behaves when it cannot connect to any Cloud Scanners, for example when no Cloud Scanner is available, or when initially working in a hotel.

Client connectivity behavior can be tuned according to company policy.

- **Disable Web access:** Web access can be blocked entirely if unable to connect to a Cloud Scanner.
- **Enable hotel mode:** Can be enabled for a restricted period.
- **Allow direct web access:** Web access can be allowed even if unable to connect to a Cloud Scanner.

Tip*:* In Hotel mode, for example for a hotel billing system or airport Wi-Fi Hotspot billing system, provide sufficient time to navigate in order to gain Internet access.
Five minutes is the recommended initial setting.

6.3.4.4 If User Cannot be Authenticated or Identified

Provides control over the level of access (risk) allowed if a user certificate is not provided when the client is installed. This can help to simplify client set-up in situations where user identification is not needed.

In addition, this can simplify set-up for demonstrations and POCs if user identification is not required.

- **Enforce:** Enables the definition of a specific security policy to be applied if no user certificate is available.
- **Allow the Mobile Security Client to send system logs:** Instructs the client to write to system logs.

6.3.5 Communications Ports - Proxies (Cloud) Tab

Note: The term **Cloud Proxy** is used in this section. **Cloud Proxy** can be used to refer to both **Cloud Scanner** and **Cloud Load Balancer.**

Tip: *SWG Management Console Reference Guide* location: Cloud Configuration in Internal Certification Mode, **Proxies (Cloud) Tab.**

6.3.5.1 Port Numbering Considerations

Tip*:* See Port Numbering Best Practice in Appendix B for details.

IMPORTANT

One very important aspect of the Hybrid that **must** be understood before attempting an implementation is IP port numbering. In SWG version 10.2 the configuration of IP port numbers was greatly simplified by providing default values (port numbering scheme), validating all port numbers to look for potential clashes and more logical screen design/layouts. The key things to remember about IP port numbers are:

1. Communications between Mobile Security Client and Cloud Scanners are always on the same ports, designated “Server Side” IP ports. There will be up to three ports, one for HTTP, one for HTTPS (if used) and a Control Port. These ports must be open on intermediate firewalls.
2. The Mobile Security Client software identifies different Cloud Scanners (e.g. one in Europe and one in the US West Coast) by internally mapping different IP port numbers to each; however, these “Local Client” port numbers are **not** used for communications to the scanners.
3. Do not confuse protocol types and port numbers, normal defaults do not apply here. All communication from the Mobile Security Client to the Cloud proxy is encrypted. So even when the client system is communicating using HTTP that traffic will be wrapped in HTTPS when travelling between the client and the Cloud Proxy. So port 443 is used by default to carry end user HTTP traffic, and port 993 has been chosen as the default for carrying end user HTTPS traffic.
4. Note that where an SWG Cloud Scanner is **not** configured to process HTTPS (perhaps the HTTPS option has not been purchased), the MSC will redirect its HTTPS traffic over the same port as HTTP to the Cloud Scanner. The HTTPS traffic will be forwarded but not scanned.

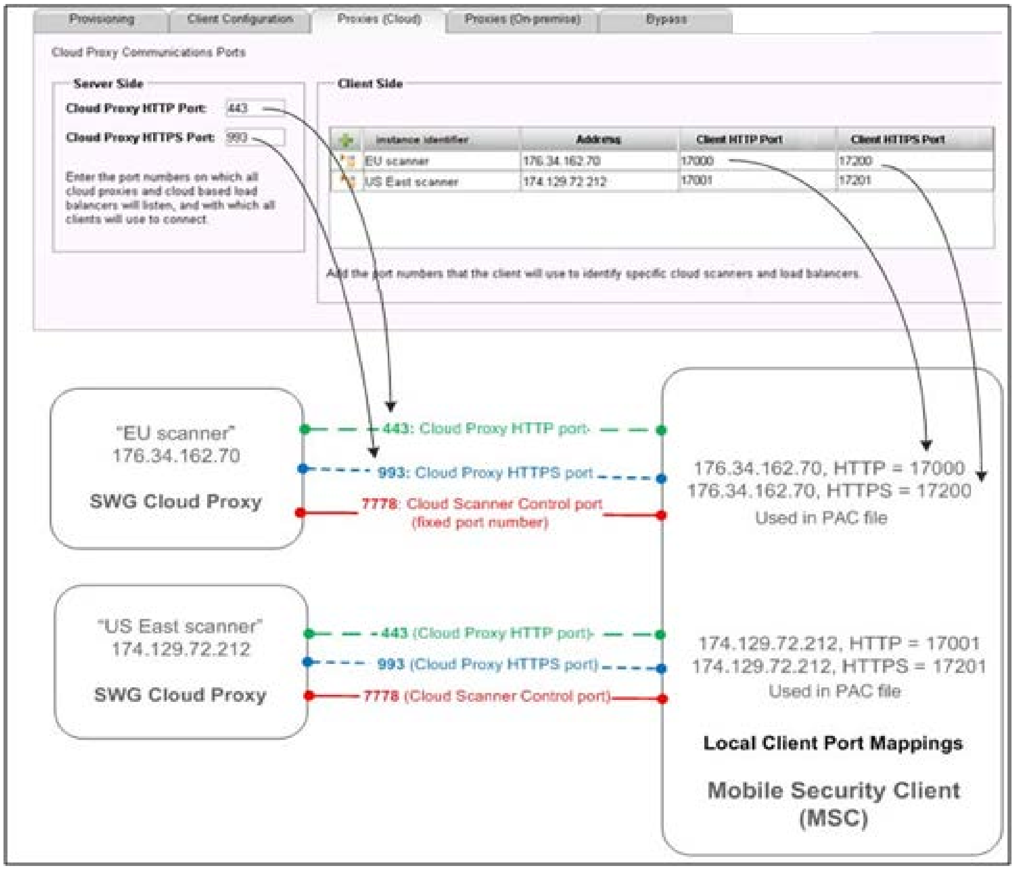
6.3.5.2 Cloud Proxy Communications Port Settings

Note: The term "Cloud Proxy" equates to "Cloud Scanner" or "Cloud Load Balancer".

The following diagram illustrates how the port numbers in the SWG Policy Server Cloud Proxy configuration screen are used in an implementation.

The scenario is that we have two Cloud Scanners in different geographic regions (Europe and the USA) and a personal computer (Windows or Mac OSX) with the Mobile Security Client installed.

IMPORTANT: The order in which Cloud Proxies are defined determines the default sequence in which they are selected during initial startup of the Mobile Security Client. In the example below, the **EU scanner** would be the default Cloud Scanner. Once latency measurements have been made by the MSC, the Cloud Scanner exhibiting the lowest latency will be used. See the *Mobile Security Client (MSC) Administrator Guide* for further details**.**



Cloud Proxy Communications Ports

Server Side

Cloud Proxy HTTP Port: 443

Cloud Proxy HTTPS Port: 993

Enter the port numbers on which all cloud proxies and cloud based load balancers will listen, and with which all clients will use to connect.

Client Side

Instance Identifier	Address	Client HTTP Port	Client HTTPS Port
EU scanner	176.34.162.70	17000	17200
US East scanner	174.129.72.212	17001	17201

Add the port numbers that the client will use to identify specific cloud scanners and load balancers.

"EU scanner"
176.34.162.70
SWG Cloud Proxy
443: Cloud Proxy HTTP port
993: Cloud Proxy HTTPS port
7778: Cloud Scanner Control port
(fixed port number)
176.34.162.70, HTTP = 17000
176.34.162.70, HTTPS = 17200
Used in PAC file
"US East scanner"
174.129.72.212
SWG Cloud Proxy
443 (Cloud Proxy HTTP port)
993 (Cloud Proxy HTTPS port)
7778 (Cloud Scanner Control port)
174.129.72.212, HTTP = 17001
174.129.72.212, HTTPS = 17201
Used in PAC file
Local Client Port Mappings
Mobile Security Client
(MSC)

Note: The Local Control Port parameter in previous SWG versions is automatically and dynamically assigned in SWG Version 11.0 and later.

Default Cloud Proxy Ports are chosen to be opportunistic. They make use of commonly open port numbers in most firewall implementations, thus reducing the amount of work required to modify the network infrastructure and also to increase the chance of being able to communicate from, for example, an airport Wi-Fi Hotspot.

6.3.6 Client Provisioning Settings - Provisioning Tab

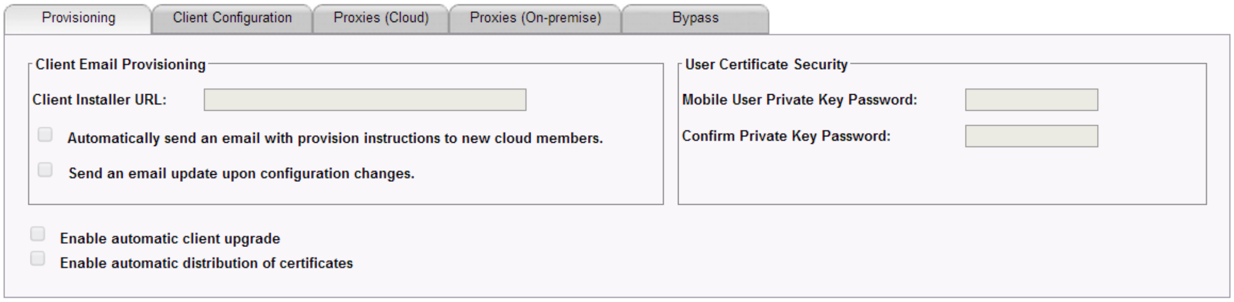
Go to **Administration | Cloud | Configuration**.

For details of fields on this screen, refer to the *SWG User Reference Guide* - Provisioning Tab section.

This screen enables increased control of the roll-out of client code (MSC) by allowing the Administrator to enable/disable automatic client code updates globally.

This is the global switch for the automatic client update feature.

For more granular control once this option is enabled, refer to Section 7.1.3, Client Code Auto-update Controlled by Group Membership.



Client Email Provisioning

Client Installer URL:

□ Automatically send an email with provision instructions to new cloud members.

□ Send an email update upon configuration changes.

User Certificate Security

Mobile User Private Key Password:

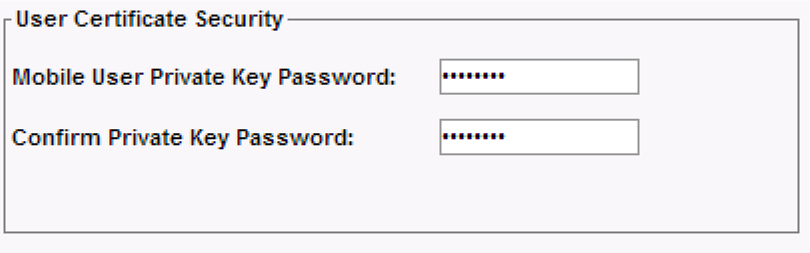
Confirm Private Key Password:

□ Enable automatic client upgrade

□ Enable automatic distribution of certificates

6.3.6.1 User Certificate Security

The **Mobile User Private Key Password** is required by end users to open their client certificates. Distribution of the password is performed manually by the administrator.



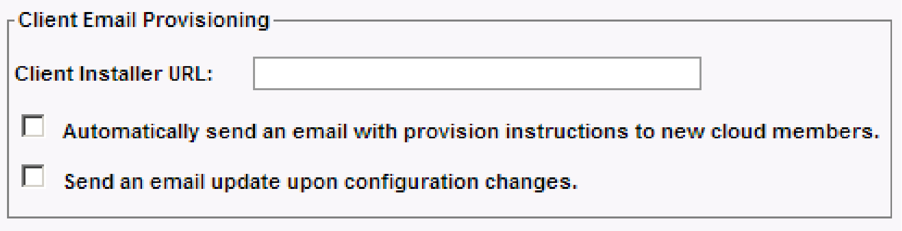
User Certificate Security

Mobile User Private Key Password: ••••••••

Confirm Private Key Password: ••••••••

6.3.6.2 Provisioning by Email Settings

A mobile user can be self-provisioned using a **Provisioning email** (see Email Template Configuration (Email Templates Screen), page 42).



Client Email Provisioning

Client Installer URL:

□ Automatically send an email with provision instructions to new cloud members.

□ Send an email update upon configuration changes.

This screen allows you to configure the Policy Server to automatically send a provisioning email to target cloud users with a link to the agent installation location, either with or without a user certificate. The user must have local administrative rights on their PC to do this.

This option is suitable for the integration phase or for small rollout/proof of concept deployment of up to a few hundred users.

- You can also choose to use the Policy Server to automatically or manually send the target user an email with the client certificate, and optionally the client installation instructions.
- Emails will only be sent after configuration, after a new certificate is issued, and after changes have been committed.

- Enabling the **Automatically send an email with provision instructions to new cloud members** check box ensures that update emails are sent to users. An update email is sent each time a new user receives new Cloud certification or a configuration change occurs.

- Enabling the **Send an email update upon configuration changes** is for existing users if changes have been made in the configuration.

The following should be configured before downloading Client Installation packages or the PAC file. It will only be possible to download the Client installer if all of the essential configuration items have been addressed:

- At least one Cloud Scanner defined
- Proxies (Cloud)
- Proxies (On-premise) optional
- Provisioning
- Bypass optional
- CA Management tab information/configuration must be completed (**Administration | Cloud | Certificate Management**). All download buttons are disabled until all relevant information is input and committed successfully.

We don't need the Mail Server to be configured, nor should we have Cloud Users or Groups. We must have CA Management, Proxies (Cloud) and Provisioning tabs configured correctly, as well as at least one Cloud Scanner before installers and PAC file are available for download.

6.3.6.3 Download PAC File

The Proxy Auto Configuration (PAC) file defines how browsers can automatically choose the appropriate proxy server for retrieving a given URL. PAC files contain a "FindProxyForURL(url, host)" function that returns a string with one or more access method specifications. These specifications cause the user to use a particular proxy server or to connect directly.

There is no need to download the PAC file unless you intend to manage it manually or have an agentless implementation (e.g. no Mobile Security clients, only remote/branch offices with Web proxies chained to the Cloud Scanners.)

- Automatic PAC File Management

  The SWG Policy Server automatically generates and maintains a PAC file based on the Cloud Configuration entered. This can be automatically updated and distributed to PCs running the Mobile Security Client.

Switch this function on by navigating to **Administration | Cloud | Configuration – Client Configuration** tab and selecting **the Enforce PAC file usage via the Mobile Security Client** option; See Client Enforcement Settings - Client Configuration Tab, page 36, for further details.

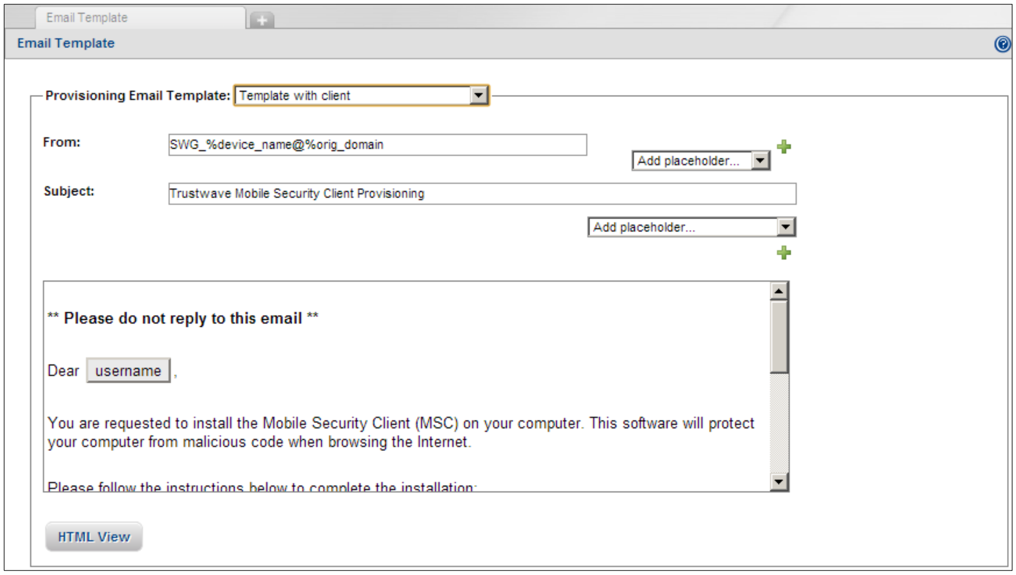
6.3.7 Email Template Configuration (Email Templates Screen)

The Secure Web Gateway provides a series of default email templates to automatically provision Cloud users via email. The templates can be customized as required, for example when using more than one client type.

To set up the provisioning email:

Go to **Administration | Cloud | Email Template**

For more information, see the *SWG Management Console Reference Guide* - Email Template section.



Provisioning Email Template: Template with client

From: SWG_%device_name@%orig_domain

Subject: Trustwave Mobile Security Client Provisioning

**** Please do not reply to this email ****

Dear username ,

You are requested to install the Mobile Security Client (MSC) on your computer. This software will protect your computer from malicious code when browsing the Internet.

Please follow the instructions below to complete the installation:

6.4 Cloud Configuration - PKI Mode

In Public Key Infrastructure (PKI) Mode, the Policy Server integrates Cloud configuration with an external Public Key Infrastructure.

When PKI Mode is used for certificate management, the Cloud Configuration screens and associated tasks change:

- Certificate Management Tab - See Certificate Management on page 32.
- Proxies (Cloud) Tab - same as Internal Certification Mode. See page 36.
- Proxies (On-premise) Tab - same as Internal Certification Mode. See page 34.
- Bypass - same as Internal Certification Mode. See page 33.

- Provisioning – See Client Provisioning Settings - Provisioning Tab on page 39.
- Client Configuration – same as Internal Certification Mode. See page 36.
- Email template – not needed in PKI Mode.

A detailed treatment of the PKI mode configuration is being constructed for this Hybrid Deployment Guide. For now, refer to the *SWG Management Console Reference Guide* for further details.

Note: Managing groups of mobile users in PKI Mode is performed by the administrator on the organization's PKI systems (assigning certificates only to mobile users). All that is required in the SWG Management Console is to import those user groups so that the SWG will be able to identify them and assign them a security policy.

6.4.1 Certificate Management

The **Certificate Management** tab is used to generate Certificates.

The top section of the tab includes:

- **CA Certificate** column — holds the relevant details of the Certificate Authority certificate, once you generate the certificate.
- **Server Certificate** column — holds the relevant details of the Server certificate, once you generate the certificate.
- **Generic Certificate** column — holds the relevant details of the Generic certificate, once you generate the certificate.

Field	Description
Common Name	Generally refers to global company name but may also reference a smaller group.
Expiration Date	Expiration date of the certificate issued.

6.4.1.1 How to Use the Certificate Management Tab

When working in the Certificate Management tab, you actually begin with the bottom section and perform the following tasks, in sequence:

1. Enter the **EKU** (Extended Key Usage) Object ID provided by the domain administrator. This property allows the client to identify the certificate with which it should connect to cloud scanners. The domain administrator defines this EKU and must use it in the certificate template from which all cloud users certificates are created.
2. Ensure the **Generate Certificates** check box is selected and click **Save** to automatically generate the CA Certificate, Server Certificate and Generic Certificate.

   The certificate details are shown in the relevant columns.

6.5 Cloud Configuration - Identification Only Mode

In Identification Only mode, the policy server acts as the Certificate Authority for the server and generic user certificates only. There is no distribution of user certificates - identity information is automatically gathered from the system for the currently logged in user.

When Identification Only Mode is used for certificate management, the Cloud Configuration screens and associated tasks change:

- **Certificate Management Tab** - same as PKI Mode. See page 32.
- **Proxies (Cloud) Tab** - same as Internal Certification Mode. See page 36.
- **Proxies (On-premise) Tab** - same as Internal Certification Mode. See page 34.
- **Bypass Tab** - same as Internal Certification Mode. See page 33.
- **Provisioning Tab** - same as PKI Mode. See page 46.
- **Client Configuration Tab** - same as Internal Certification Mode. See page 36.
- **Email template** - not needed in Identification Mode.

For more information, refer to the *SWG Management Console Reference Guide.*

6.6 User Management

6.6.1 Cloud Users and Groups (Internal Certification Mode)

This section is relevant to cloud implementation only in **Internal Certification Mode,** as we can detect new users in Cloud groups and assign them certificates and send a provisioning email. In PKI Mode and Identification Only Mode this has no bearing.

User Groups can be created locally on the SWG or imported from LDAP. Using LDAP is recommended since it makes it possible for changes in, for example, Active Directory group membership to be reflected automatically in the SWG. That is, new joiners to an organization will automatically be added, and leavers will be removed.

The key Cloud related parameters which must be configured for the group are:

- Select **Issue Mobile Security Client Certificates to new group members** to automate certificate distribution.
- Select **Prevent user from disabling Mobile Security Client** if you wish to prevent the users in this group from being able to temporarily disable the client software. This function is typically for trusted users.

6.6.1.1 User Defined User Groups

To modify User Defined User Groups settings for Cloud, navigate to **Users | Users / User Groups** then click the particular group node.

For details of how to configure user groups and LDAP, refer for the *SWG User Reference Guide.*

6.6.1.2 LDAP Groups

To modify LDAP group settings for Cloud, navigate to **Users | LDAP** and select the particular LDAP Group node.

For details of how to configure Directory Groups for Cloud Users, refer to the *SWG User Reference Guide*.

6.6.2 Client Certificate Management (Internal Certification Mode)

See **Internal Certification Mode – Internal Email Distribution of Certificates**, page 47.

7 Deploying Mobile Security Client and Certificates

This section is provided to help guide the Administrator through the activities of MSC and Certificate deployment.

7.1 Client Deployment

Options for deployment of the Mobile Security Client software are discussed in Section 4.5, Client deployment method choice: email or external system?

7.1.1 Internal Certification Mode Email Distribution of Client

To configure the SWG to deploy the MSC by SWG "internal" email-delivered link direct to the end user, see Client Provisioning Settings - Provisioning Tab, page 39.

Note: Using the Internal Certification Mode email distribution method also assumes that the client certificates will be delivered by email from the SWG Policy Server.

7.1.2 Active Directory/Group Policy Object Based Deployment of Client

To deploy the MSC using an external software distribution mechanism, such as MS Active Directory and Group Policy Objects, you will need to:

1. Download the client installers required.

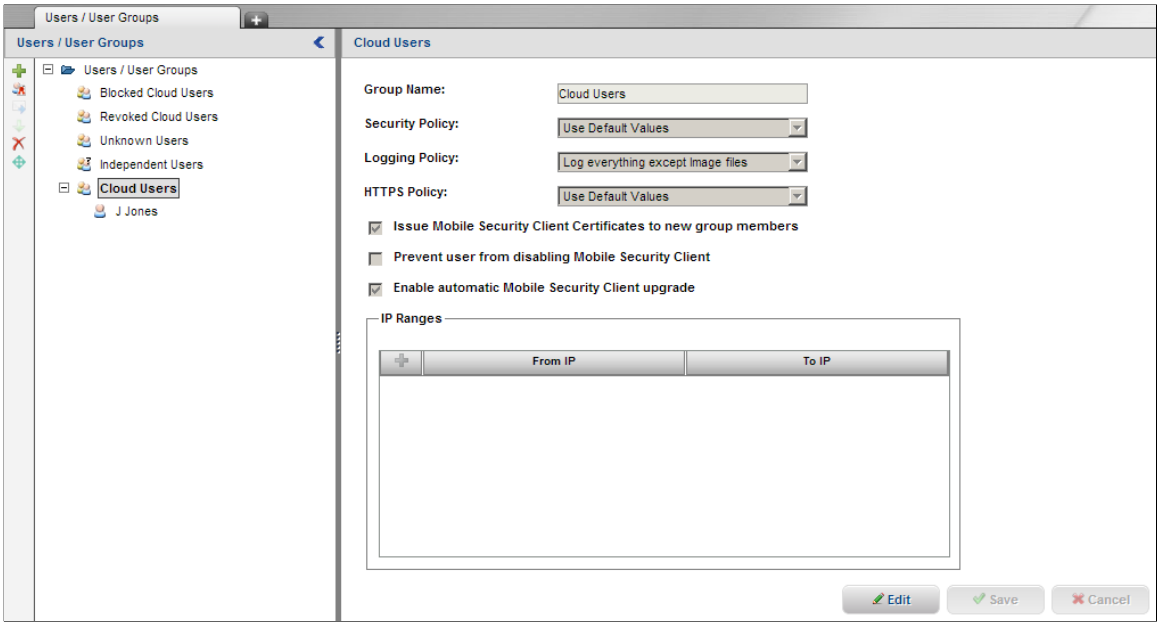
2. Follow the AD/GPO instructions in Appendix A - AD MSC Installer Distribution.

7.1.3 Client Code Auto-update Controlled by Group Membership

Client code auto-updates can be controlled by group membership, allowing the administrator to update MSC code by user group, and enabling the phased roll-out of new MSC versions. This feature must first be enabled globally by selecting the **Enable automatic client upgrade** check box in **Administration | Cloud | Configuration** – Provisioning tab.

Sales Engineers can also restrict MSC roll-out of new versions for test, pilot, or POC purposes.

For more information, see Deployment Decisions and Preparation, page 19.



Group Name: Cloud Users

Security Policy: Use Default Values

Logging Policy: Log everything except Image files

HTTPS Policy: Use Default Values

☑ Issue Mobile Security Client Certificates to new group members

☐ Prevent user from disabling Mobile Security Client

☑ Enable automatic Mobile Security Client upgrade

IP Ranges

From IP	To IP

7.2 Certificate Deployment

Options for Certificate management are discussed in Section 4.3, Certificate management method choice: PKI Mode or Internal Certification Mode? Depending on your choice of certificate management method, use the appropriate section below.

7.2.1 Automatic Distribution of Certificates

To configure that certificates are distributed from the scanner to the mobile security client automatically:

Select the **Enable automatic Distribution of Certificates check** box in **Administration | Cloud | Configuration** – Provisioning tab.

7.2.2 PKI Mode (External PKI System)

To configure for PKI mode, see the Workflow Table in Work Flow for Configuring the SWG Policy Server for Hybrid Deployment, page 26.

7.2.3 Internal Certification Mode – Internal Email Distribution of Certificates

The following sections are provided as a quick reference. For more detailed instructions on issuing Client Certificates by groups, domains and individual users see the Users chapter of the *SWG Management Console Reference Guide*.

7.2.3.1 Issue Certificate to Users and Groups Automatically

To issue Cloud certificates to Users and Groups:

1. Navigate to **Users | Users/User Groups**.
2. Enable the **Issue Mobile Security Client Cloud Certificate to new group members** check box.

Note: This section relies on previously configured domain users. For more information on domain users and local users, refer to the *SWG User Reference Guide* on Adding Domain Users.

Client certificates will then automatically be issued to new group members.

7.2.3.2 Issue Certificates to Domain Users Automatically

To issue Cloud certificates for domain users:

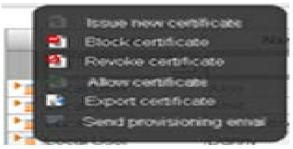
1. Navigate to **Users | LDAP**.
2. Right-click the LDAP directory and select the required LDAP group.
3. Click **Edit** and then enable the check box in the screen.

Client certificates will then automatically be issued to new group members.

7.2.3.3 Issue Certificates to Individual Users Manually

To issue Cloud certificates per User:

1. Navigate to **Users | User Grouping and Certificate Management**.
2. Select the particular cloud user for whom a certificate is to be issued.
3. Click the icon, then select **Issue new certificate**.

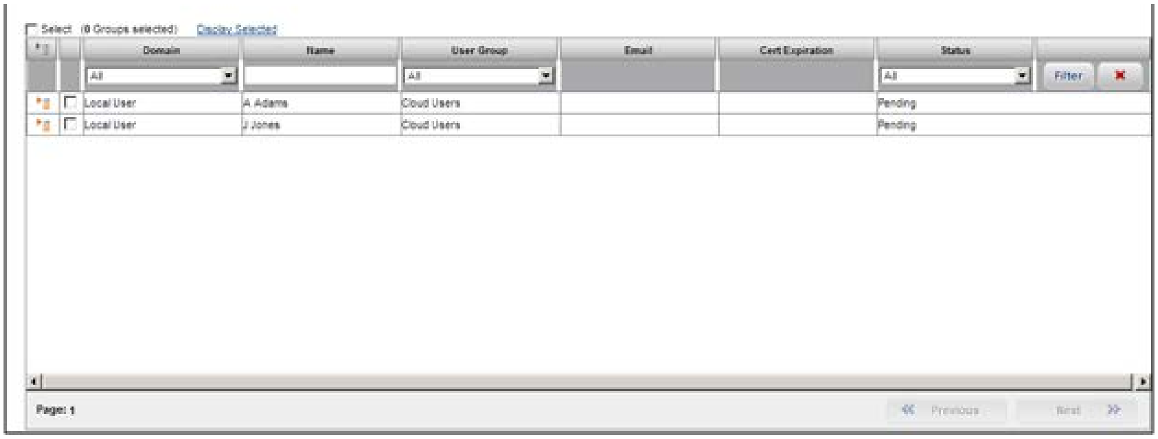


A client certificate will be sent via email to the selected user.

7.2.4 Manage User Certificates for Multiple Users

Go to **Users | User Grouping and Certificate Management**.

User certificate management actions such as issue, revoke, and so on can be performed concurrently on multiple users based on selection criteria, including group names.



□ Select (0 Groups selected) Display Selected

		Domain	Name	User Group	Email	Cert Expiration	Status	
		All		All			All	Filter ✖
	□	Local User	A Adams	Cloud Users			Pending	
	□	Local User	J Jones	Cloud Users			Pending	

Page: 1

7.2.5 Automatic Distribution of Certificates

To configure that certificates are distributed from the scanner to the mobile security client automatically:

Select the **Enable automatic Distribution of Certificates check** box in **Administration | Cloud | Configuration** – Provisioning tab.

7.2.6 Issue Certificates via Active Directory Distribution

The following steps are needed:

Export all client certificates from SWG for use in Active Directory:

1. Login to the SWG Management Console and navigate to **Users | User Grouping and Certificate Management**.
2. Click the **Export All Certificates** button.
3. Save the export file.

The export file will contain all valid client certificates arranged in a zipped directory structure organized by folders representing the user groups (defined in the **Users | User Groups** screen).

Use this file as input to the Active Directory/Group Policy Object distribution process.

To import the client certificate files into the Active Directory:

See Appendix A – AD Certificate Distribution.

Appendix A – Active Directory Distribution

AD Certificate Distribution

Important: Trustwave makes no representations or warranties of any nature regarding the third party tools/products, scripts/script files referenced herein. Your use of such third party tools/products, scripts/script files is entirely at your own risk, and you agree Trustwave shall have no liability resulting therefrom.

The following is a suggested solution for the distribution of the **Client Certificates** (.p12) via the organization's Active Directory Group Policy Objects (GPO). It consists of a silent installation and distribution of digital certificates as a unique identifier for end-users of the Trustwave SWG-Hybrid deployment with Cloud Scanners.

On user login to the domain, on a station in which the Mobile Security Client is already installed, the user will receive the unique key and certificate via the domain's GPO. It should be noted that this solution will be applied at the user's login (not when unlocked) and when the policy is refreshed (based on the set defaults of the organization). The Solution will test whether the certificate is needed, and if so, the certificate will be installed for the user.

Preparation

To obtain the script files:

1. Download and install a file archive manager, such as 7-zip (www.7-zip.org).
2. Define a dedicated file folder in the system where cloud user certificates are to be placed (for example: CertsDir).
3. Extract the cloud user certificates, as downloaded from the SWG Policy Server GUI [insert exact screen name and documentation reference], into CertsDir.
   Ensure the certificate name format is as follows: <username>.p12
4. Extract both **ChangePermissions.bat** and **Install.vbs** script files to the CertsDir (obtain Trustwave SWS-AD Integration.zip file or create the scripts from the details provided in the section **Active Directory Integration Scripts** below).
5. Run the **ChangePermissions.bat** file (The file should be run under Administrator privileges).

Note: The .bat file changes the permissions on the certificate (.p12) files and allows each user to access only the certificate file that belongs uniquely to that user.

To edit the script variables according to the enterprise-specific environment:

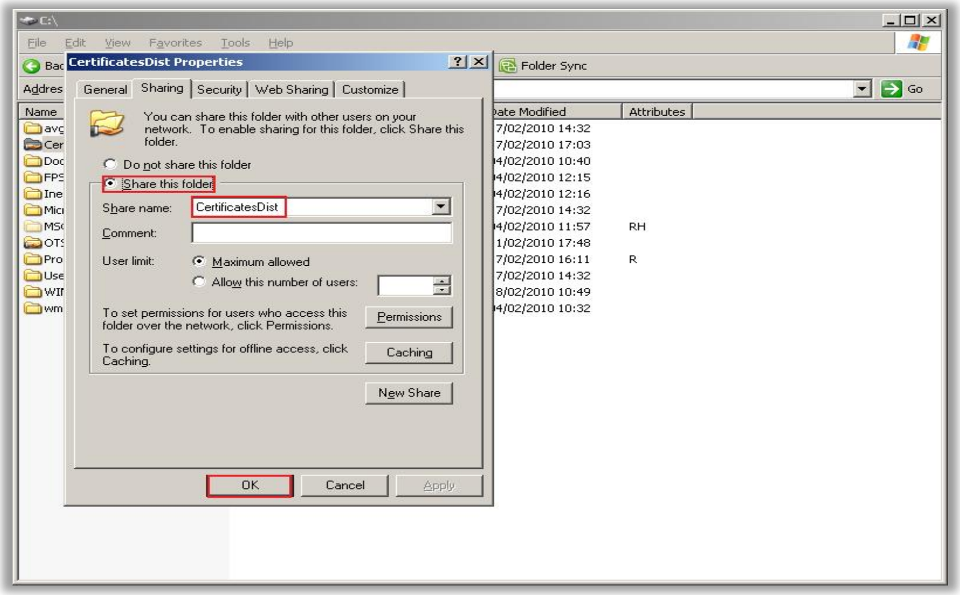
1. Right-click the file **Install.vbs** and select **Edit.**
2. In the selected text, change the values for the following:
   - SERVER – The server from which the cloud users obtain their certificates.
   - PASSWORD – The cloud user's certificate password as defined in the Policy Server GUI during initial policy server configurations.

Note: "The server" pertains to the Domain Controller IP/name and not the Policy Server name.

3. Save the file and exit.

Server Actions

1. Create a folder titled "**CertificatesDist**". This folder can be created anywhere in the file system of the operating system.
2. Right-click the **CertificatesDist** folder and select **Sharing and Security**.
3. Enable the **Share this folder** radio button and set the share name as **CertificatesDist**.



CertificatesDist Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: CertificatesDist

Comment:

User limit: ● Maximum allowed

○ Allow this number of users:

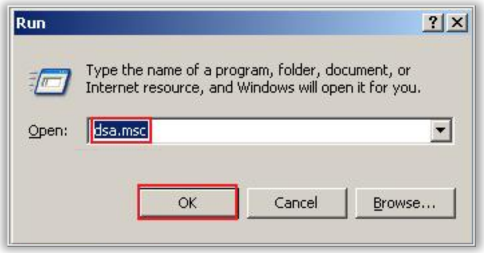
To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

4. Move all the files previously created in the Preparation section above, as well as the certificate files, to the **CertificatesDist** folder.

Active Directory Actions

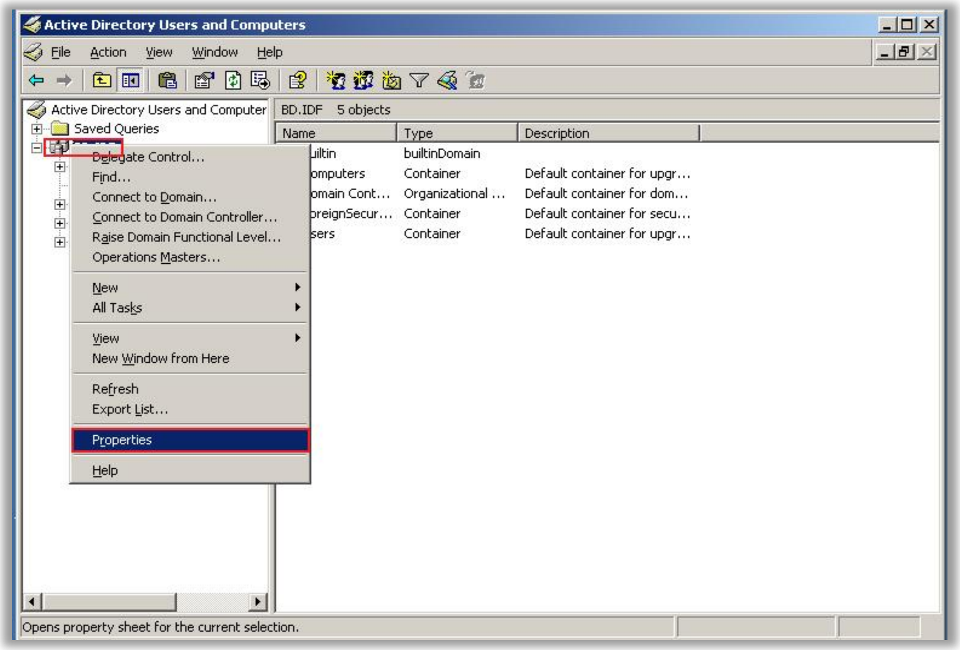
1. Open the Active Directory Users and Computers management screen.
    a. Navigate to the Start menu, select **Run**.
    b. Enter line: **dsa.msc** and click **OK.**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dsa.msc

The Active Directory Users and Computers screen opens:



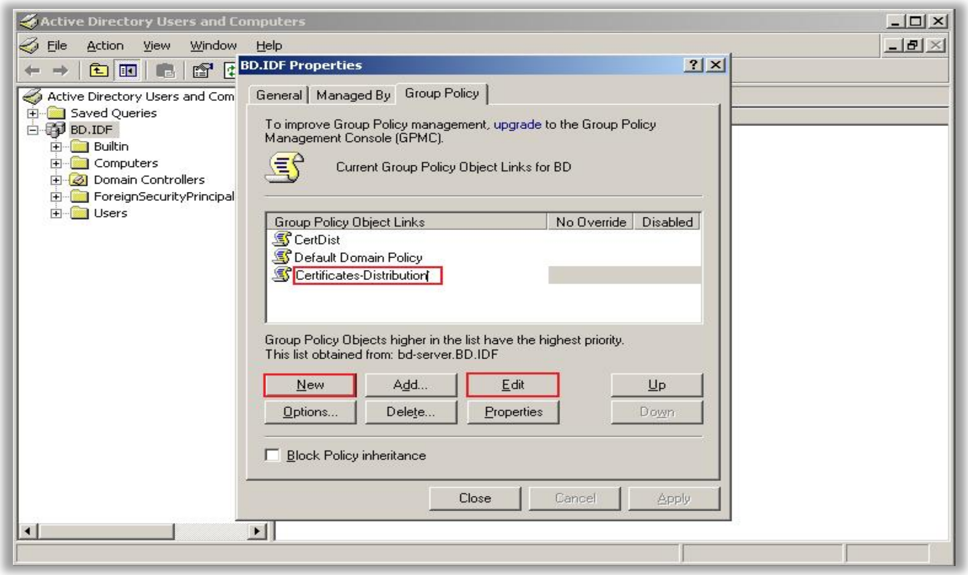
BD.IDF 5 objects

Name	Type	Description
uiltin	builtinDomain	
omputers	Container	Default container for upgr...
omain Cont...	Organizational ...	Default container for dom...
oreignSecur...	Container	Default container for secu...
sers	Container	Default container for upgr...

Opens property sheet for the current selection.

2. In the left tree pane, select the **Domain**, right-click and choose **Properties**.
3. In the **Domain Properties** window, in the **Group Policy** tab, create the required Group Policy Object:
    a. Click **New**.
    b. Change the name of the Group Policy Object as required. For example: **Certificates-Distribution**.

c. Click **Edit.**



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for BD

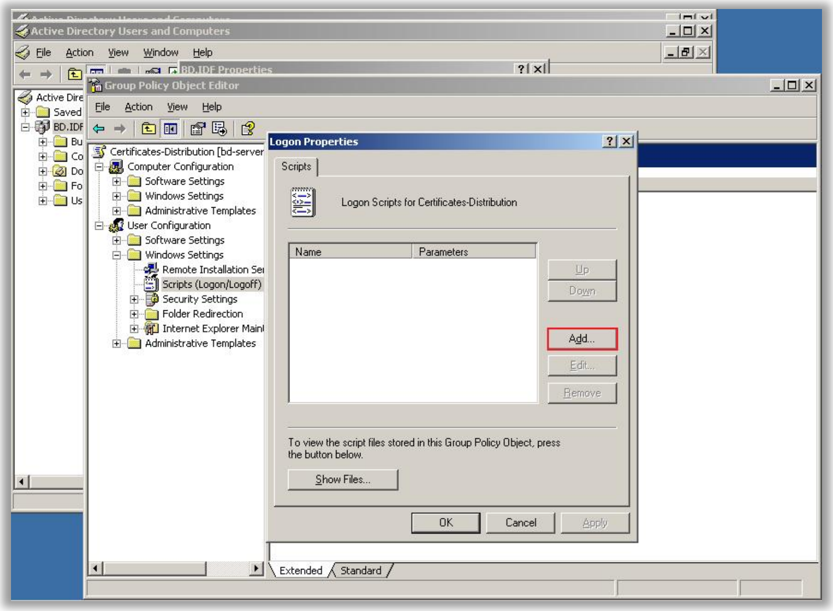
Group Policy Object Links	No Override	Disabled
CertDist		
Default Domain Policy		
Certificates-Distribution		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: bd-server.BD.IDF

d. In the open Group Policy Object Editor window, navigate to **Windows Settings.**

e. Select **Scripts (Logon /Logoff)** and double-click **Logon**.

f. Click **Add.**



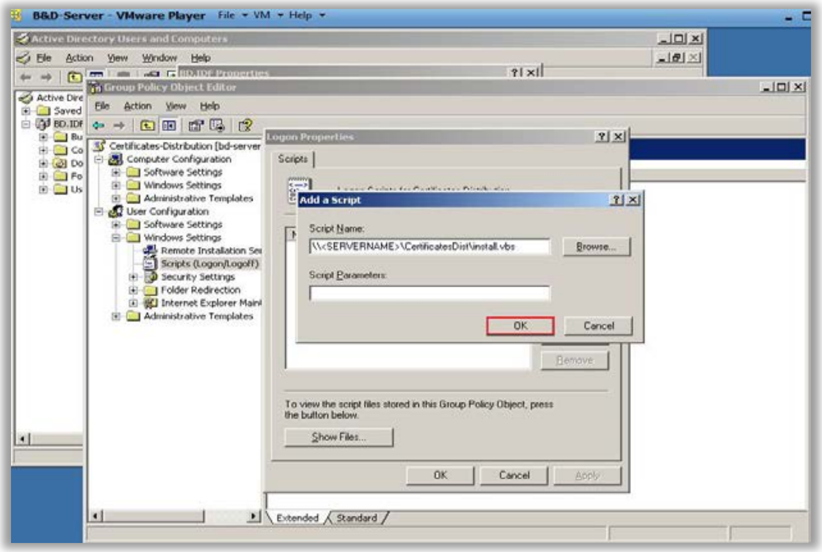
Logon Scripts for Certificates-Distribution

Name	Parameters

To view the script files stored in this Group Policy Object, press the button below.

g. Under **Script Name**, register the full path of the share folder where the script **Install.vbs** is saved, and click **OK.** The path should be, for example, \\<SERVERNAME>\CertificatesDist\install.vbs

WARNING! Do not choose the path via Browse. Enter the path manually.



Script Name: \\<SERVERNAME>\CertificatesDist\install.vbs

Script Parameters:

To view the script files stored in this Group Policy Object, press the button below.

h. In the Logon Properties window, click **OK.**

i. Close the Group Policy Object Editor window.

4. In the **Properties** window (Domain), click **Close**.
5. Close the Active Directory Users and Computers management screen.
6. Click **Start**, select **Run**, and enter "**gpupdate/force**" in the text box.
7. Click **OK**.

Active Directory Integration Scripts

M86SWS-AD-Integration.zip

Obtain the Active Directory integration utility scripts from the Trustwave Knowledge Base/Support Web site, or create the required scripts based on the text below:

Change Permissions (Windows Batch File)

```
dir /b *.p12 > p12s.txt

for /f %%a IN (p12s.txt) do Echo Y| cacls %%~na.p12 /t /c /g %%~na:F

del p12s.txt
```

Install (VBScript Script File)

```
Dim PASSWORD, SERVER, USER, TEMPDIR, PROGDIR

PASSWORD = "12345"

SERVER = "192.168.90.64"

USER = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%username%")

TEMPDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%")

PROGDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%ProgramFiles%")


set FSO = CreateObject("Scripting.FileSystemObject")

If FSO.FileExists( PROGDIR & "\Finjan\FCS Agent\fcsagent.exe") Then

        If  FSO.FileExists("\\" & SERVER & "\CertificatesDist" & "\" & USER & ".p12") Then

                Dim objFSO, WSHNetwork

                Const OverWriteExisting = True

                Set objFSO = Createobject("Scripting.FileSystemObject")

                wsLocation = TEMPDIR & "\"

                objFSO.CopyFile "\\" & SERVER & "\CertificatesDist" & "\" & USER & ".p12", wsLocation, OverWriteExisting


                strProgramPath = PROGDIR & "\Finjan\FCS Agent\CertificateImporter.exe"

                set objShell = createobject("Wscript.Shell")

                objShell.Run Chr(34) & strProgramPath & Chr(34) & " " & wsLocation & USER & ".p12" & " " & PASSWORD, 1, true


                Set aFile = fso.GetFile(TEMPDIR & "\" & USER & ".p12")

                aFile.Delete

        End If

End If
```

AD MSC Installer Distribution

Trustwave provides a solution for the distribution of the Mobile Security Client via the organizations Active Directory Group Policy Objects (GPO). The solution is a silent installation of the Mobile Security Client for end-users of the Trustwave SWG-Hybrid deployment with Cloud Scanners.

To install the Agent, an administrator must log into the work station/PC. This is required as the agent must be installed with administrator privileges.

Preparation

To obtain the script files:

1. Download and install any file archive manager, such as 7-zip (www.7-zip.com).
2. Define a dedicated file folder in the system where MSC installer is to be placed (for example: MSCInstallerDir).
3. Download the MSC installer from the SWG Policy Server GUI [insert exact screen name and documentation reference], into MSCInstallerDir. **The Installer name can be changed!!**
4. Extract the **installAgent.vbs** script file to the MSCInstallerDir (obtain Trustwave SWS-AD Integration.zip file or create the script from the details provided in the section **Active Directory Integration Scripts** below).

To edit the script variables according to the enterprise-specific environment:

1. Right-click the file **InstallAgent.vbs** and select **Edit**.
2. In the selected text, change the values for the following:
    - SERVER – The server from which the cloud users obtain their certificates.

Note: The "server" pertains to the Domain Controller IP/name and not the Policy Server name.

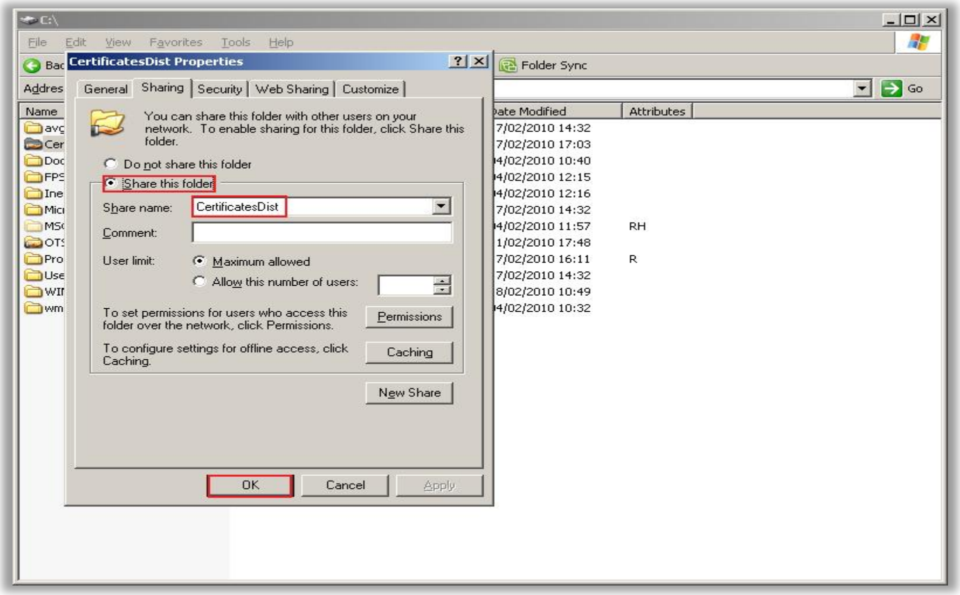
    - INSTALLER – The Secure Web Service Agent installer file name. The installer is downloaded from the Policy Server GUI.

3. Save the file and exit.

Server Actions

1. Create a folder titled "**ClientDist**". This folder can be created anywhere in the file system of the operating system.
2. Right-click the **ClientDist** folder and select **Sharing and Security**.

3. Enable the **Share this folder** radio button and set the share name as ClientDist.



CertificatesDist Properties

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder
● Share this folder

Share name: CertificatesDist

Comment:

User limit: ● Maximum allowed
○ Allow this number of users:

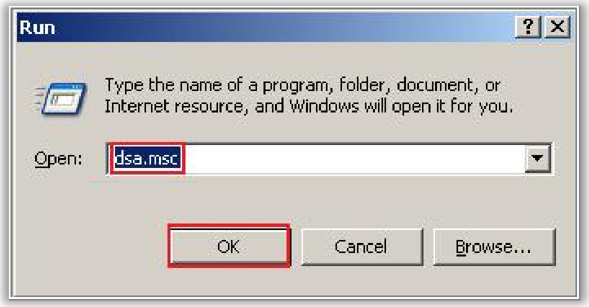
To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

4. Move all the files previously created in the Preparation section above, as well as the MSC installer, to the **ClientDist** folder.

Active Directory Actions

1. Open the Active Directory Users and Computers management screen.
   a. Navigate to the Start menu, select **Run**.
   b. Enter line: **dsa.msc** and click **OK**.

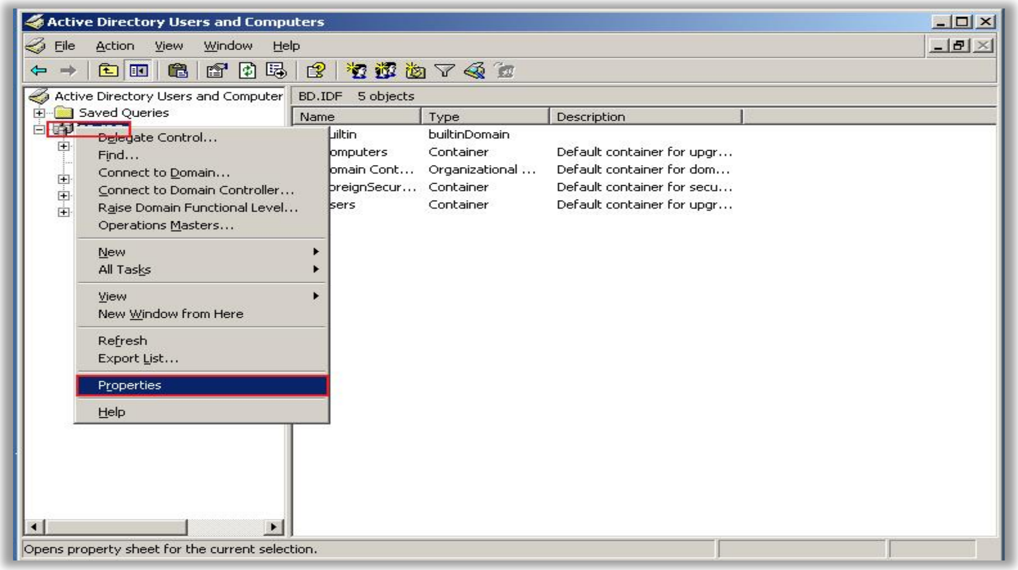


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dsa.msc

The Active Directory Users and Computers screen opens:

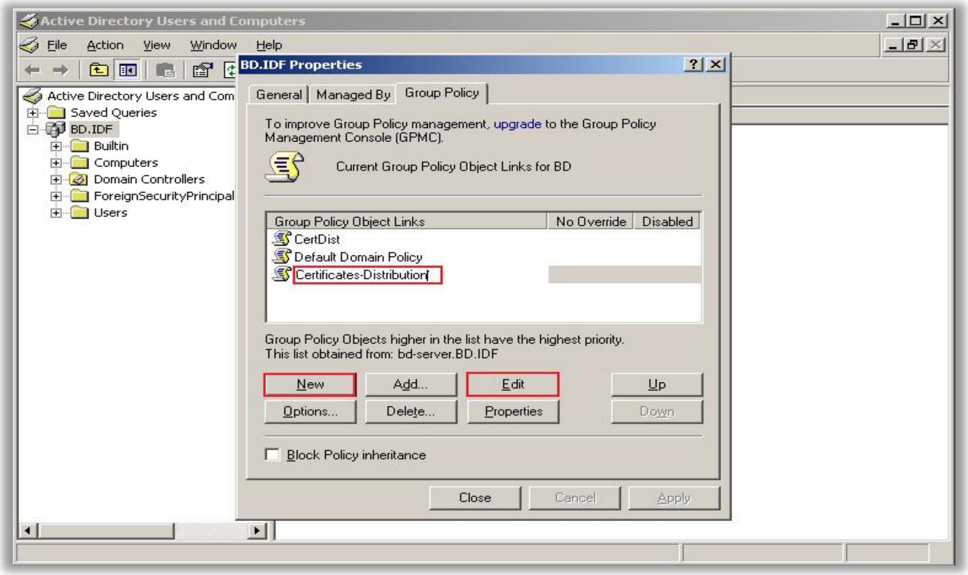

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
Delegate Control...
Find...
Connect to Domain...
Connect to Domain Controller...
Raise Domain Functional Level...
Operations Masters...
New
All Tasks
View
New Window from Here
Refresh
Export List...
Properties
Help

BD.IDF 5 objects

Name	Type	Description
uiltin	builtinDomain	
omputers	Container	Default container for upgr...
omain Cont...	Organizational ...	Default container for dom...
oreignSecur...	Container	Default container for secu...
sers	Container	Default container for upgr...

Opens property sheet for the current selection.

2. In the left tree pane, select the **Domain**, right-click and choose **Properties**.
3. In the **Domain Properties** window, in the **Group Policy** tab, create the required Group Policy Object:
   a. Click **New**.
   b. Change the name of the Group Policy Object as required. For example: MSC-Distribution.
   c. Click **Edit**.



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for BD

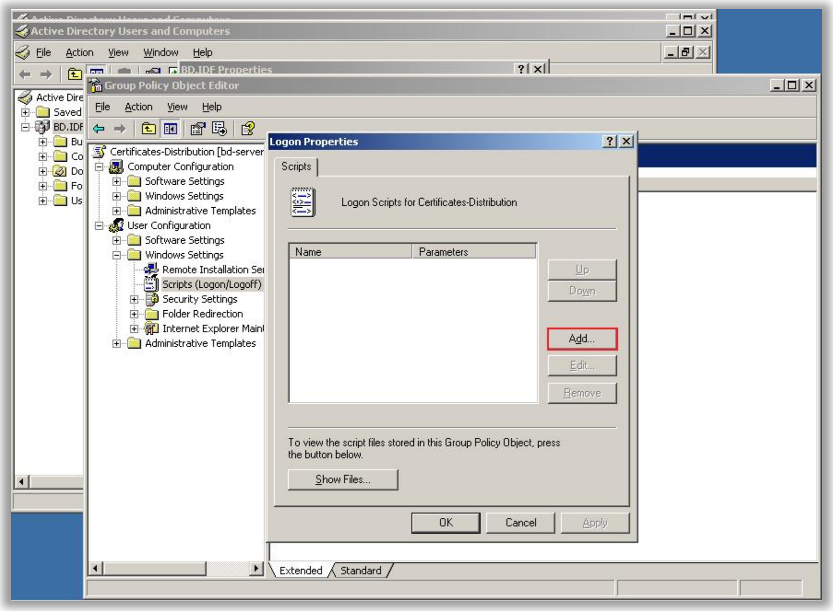
Group Policy Object Links	No Override	Disabled
CertDist		
Default Domain Policy		
Certificates-Distribution		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: bd-server.BD.IDF

□ Block Policy inheritance

   d. In the open Group Policy Object Editor window, navigate to **Windows Settings**.
   e. Select **Scripts (Logon /Logoff)** and double-click **Logon**.

f. Click **Add**.



Logon Scripts for Certificates-Distribution

To view the script files stored in this Group Policy Object, press the button below.

g. Under **Script Name**, enter the full path of the share folder where the script **InstallAgent.vbs** is saved and click **OK**.

WARNING! Do not choose the path via Browse. Enter the path manually.

h. In the Logon Properties window, click **OK**.

i. Close the Group Policy Object Editor window.

4. In the **Properties** window (Domain), click **Close**.
5. Close Active Directory Users and Computers.
6. Click **Start**, select **Run**, and enter "**gpupdate /force**" in the text box.
7. Click **OK**.

Active Directory Integration Scripts

M86SWS-AD-Integration.zip

To obtain the Active Directory integration utility scripts, either contact Trustwave Technical Support or create the required scripts based on the text below.

Obtain the Active Directory integration utility scripts from the Trustwave Knowledge Base/Support Web site or create the required scripts based on the text below.

installAgent (VBScript Script File)

```
Dim SERVER, INSTALLER, USER, TEMPDIR, PROGDIR
SERVER = "192.168.90.64"
INSTALLER = "SWSA.exe"
USER = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%username%")
TEMPDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%")
PROGDIR = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%ProgramFiles%")

set FSO = CreateObject("Scripting.FileSystemObject")
If FSO.FileExists(PROGDIR  & "\Finjan\fcs agent\fcsagent.conf") Then
        wscript.quit
End If

If StrComp(USER, "administrator", vbTextCompare) = 0 Then
        Dim objFSO
        Set objFSO = CreateObject("Scripting.FileSystemObject")
        objFSO.CopyFile "\\" & SERVER & "\CertificatesDist\" & INSTALLER, TEMPDIR & "\", True
        strProgramPath = TEMPDIR & "\" & INSTALLER
        set objShell = createobject("Wscript.Shell")
        objShell.Run strProgramPath & " /S"
End If
```

Appendix B – Port Numbering Best Practice

All Cloud configuration port numbers are customisable by the administrator; however the defaults have been chosen to give best results in most situations.

Tips:

- Windows PCs and Mac PCs are no different when it comes to port configuration.
- An Amazon EC2 Cloud Scanner looks the same to the SWG Policy Server as a Trustwave SWS-Hybrid Cloud Scanner.
- To make the configuration self-documenting, we suggest that the comment field "**Cloud Instance Identifier**" is used to identify the type and location of the Cloud Scanner device. This can also be linked to the Amazon EC2 Instance name.

In the example configuration data below, both HTTP and HTTPS are being used. In addition, the "IP Address" is the IP address of the Cloud Scanner or Load Balancer.

CONTROL PORT	27778		
SERVER SIDE			
Cloud Proxy HTTP Port	443		
Cloud Proxy HTTPS Port	993		
CLIENT SIDE		**Local Client**	
Comment	**IP Address**	**HTTP Port**	**HTTPS Port**
Cloud Scanner 1 (e.g. USA)	n.n.n.a	17000	17200
Cloud Scanner 2 (e.g. Europe)	n.n.n.b	17001	17201
Cloud scanner x	n.n.n.c	1700x	1720x

Appendix C – Useful Links

- PAC file resource: http://findproxyforurl.com/iphone_proxy_pac.html
- Amazon EC2 FAQs: http://aws.amazon.com/ec2/faqs/
- Trustwave SWG Documentation: http://www.Trustwave.com/support/Secure-Web-Gateway/Documentation.asp

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide.

For more information, visit https://www.trustwave.com.